

Document Title	Product security Risk Table
Document number / Revision	D001020017 / 02
Date	21-Aug-22
Project	SmartMedic Phase II
Project number	SGTC-NPD-001

		Product Security Risk Ta	ble approval	
Approvals	Name	Title	Signature	Date
Author	Deepak Sharma	Design Engineering R&D (Software)		
	Ashish Gaurav	V&V Lead		
Approvers	Vikram Puri	Advanced Operations (Mfg & QA)		
	Sreejith Viswam	Advance Quality Engineer		

Document Revision History:

REV#	Revision Date	Author	Description of Revision
00	30-Aug-21	Deepak Sharma	Initial Release DR1-4 Document was reviewed but not approved and archived, thus archiving
01	8-Apr-22	Deepak Sharma	Document updated as per DR5-7 requirements -Security Controls/Mitigations -Security Risk Control Measures -Implementation of Risk Control Measures -Verification of Risk Control Measures (Effectiveness)
02	21-Aug-22	Deepak Sharma	DR8-10 updates Security Ris Assess Tab -Security Penetration Test Report: D001020164 reference no. added in Verification of Risk Control Measures (Effectiveness) -Mapping in Verification of Risk Control Measures (Effectiveness) modified as per VAPT Testcases -SOM mapping updated as per the SOM Document D001020115 -Residual Security Risk Acceptability Justification updated for No reisudal risk -Remarks (Column added additionaly for SOM Reference in Security Risk Assess Tab

Stryker Confidential Page 1 of 29

Doc Number: D000000909 Name: Product Security Risk Table

Revision: AB Form

System & Asset Identification

Medical Device / System:	SmartMedic
Scope:	SmartMedic -001-02-A-00-00
Date:	21-Aug-22
Conducted by:	<author function="" name="" organization=""> Deepak Sharma / Design Engineering R&D Software</author>

ID#	Asset Type (Information/Physical)	Asset	Asset Description
A01	Physical Asset	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	Utilizing computer resources and computing power by adversary, allows various general purpose attacks, such as incl. Ransomware deployment, Bitcoin Mining, abuse of peripheral devices such as WebCam, Microphones, etc., .
A02	Information asset	Tablet OS/network details & Tablet Application	Information about internals of the system (Device identification, software versions, supported protocols, etc.)
A03	Physical Assets	Smart medic (Stryker device) System Component	Monitors local bed status information, alerting caregivers visually, audibly or remotely if preset parameters are compromised.
A04	Information asset	Authentication/Authorisation method of all device(s)/app	Information related to authenication/authorisation data (password/pins/MFA/Biometrics)
A05	Physical Assets	Device Maintainence tool (Hardware/Software)	Device Maintainence tool (Hardware/Software) that patchs and updates Smart Medic Device and Application related to Security
A06	Information asset	Electronic Health Records (EHR)/ Device Component status	Smart device components health status information
A07	Information asset	Interface/API Communication	Communication middleware enables communication and data management for distributed applications.
A08	Physical Assets	Wireless Network device (Scope of HDO)	Devices that are used for communication among the Smart Medic project component.
A09	Information asset	Data at Rest	Use strong encryption algorthim to store data on cloud platform (Smartmedic Device)/tablet
A10	Information asset	Data in Transit	Use strong encryption algorthim to data moving on tablet to cloud platform(Smartmedic Device)/tablet
A11	Information asset	Smart medic app (Stryker Admin Web Application)	Smart medic application for nurse/health worker (Stryker Admin Web Application)
A12	Information asset	Smart medic app (Azure Portal Administrator)	Azure Portal Administrator for Smart medic app
A13	Information asset	Azure Cloud DataBase	Azure Cloud DataBase related to Smart Medic app
A14	Information asset	Health vital data	Health vital data Body temperature. Pulse rate. Respiration rate, weight data, position data, etc.
A15	Information asset	Nurse Station Application	Smart medic web application for nurse/health worker running on the Nurse Station

Printed copies for reference only

Stryker Confidential - This document contains information that is confidential and proprietary. Neither this document nor the information herein may be reproduced, used, or disclosed to or for the benefit of any third party without the prior written consent of Stryker.

D05788-1, Ver 1

Stryker Confidential Page 2 of 29

Doc Number: D000000909

Name: Product Security Risk Table

Revision: AB Form

Vulnerability Identification

Vuln. ID	Vulnerability Description	Applicable (Yes/No)	Rationale (if Vulnerability not applicable)
V01	Devices with default passwords needs to be checked for bruteforce	Yes	n/a
	attacks		
V02	External communications and exposure for communciation channels	Yes	n/a
	from and to application and devices like tablet and smartmedic device.		
V03	The password complexity or location vulnerability. Like weak	Yes	n/a
	passwords and hardcoded passwords.		
V04	Checking authentication modes for possible hacks and bypasses	Yes	n/a
V05	Insecure communications in networks (hospital)	Yes	n/a
SBOM			
<u>V06</u>	Lack of Asset location digaram in security operations manual	Yes	n/a
V07	Lack of configuration controls for IT assets in the informaion system plan	Yes	n/a
V08	Ineffective patch management of firware, OS and applications	Yes	n/a
	thoughout the information system plan		' ·
V09	Lack of plan for periodic Software Vulnerability Management	Yes	n/a
V10	The static connection digaram between devices and applications with		n/a
	provision for periodic updation as per changes		·
V11	Assest counting system for all instances of product implementation	Yes	n/a
Access points			
V12	Unprotected network port(s) on network devices and connection	Yes	n/a
	points		
V13	Unprotected external USB Port on the tablet/devices.	Yes	n/a
V14	Unencrypted Network segment through out the information flow	Yes	n/a
V15	Controlled Use of Administrative Privileges over the network	Yes	n/a
Data			
V16	Unencrypted data at rest in all possible locations	Yes	n/a
V17	Unencrypted data in transit in all flowchannels	Yes	n/a
V18	Weak Encryption Implementaion in data at rest and in transit tactical and design wise	Yes	n/a
V19	Weak Algorthim implementation with respect cipher key size	Yes	n/a
InSecure Configurations of Resources			
V20	InSecure/not recommended Configuration for Mobile Devices,	Yes	n/a
	Laptops, Workstations, and Servers		
V21	InSecure Configuration for Software/OS on Mobile Devices, Laptops,	Yes	n/a
	Workstations, and Servers		
V22	Legacy system identification if any	Yes	n/a
V23	Outdated - Software/Hardware	Yes	n/a
V31	Improper/insufficient provisioning of IOT hub	Yes	n/a
V32	Unsecured communication with unauthenticated 3rd party devices	Yes	n/a
AuthN management			
V24	Error Info containing sensitive data for Failed Authentication attempts	Yes	n/a
V25	Absence of additional security factor along with user identification	Yes	n/a
V26	Having no limit on the login attempts	Yes	n/a
V27	No session expiry after certain time interval	Yes	n/a
Logging/Monitoring		••	,
V28	Insufficient Logging information	Yes	n/a
V29	Insufficient Access permissions for accessing and modifying Log files	Yes	n/a
Keys & Certificates			
V30	Improper security (for ex., Storage & Access) for Key tokens and	Yes	n/a
	Certificates		

Printed copies for reference only

Stryker Confidential - This document contains information that is confidential and proprietary. Neither this document nor the information herein may be reproduced, used, or disclosed to or for the benefit of any third party without the prior written consent of Stryker.

Stryker Confidential Page 3 of 29

Doc Number: D000000909
Name: Product Security Risk Table

Revision: AB Form

Threat Assessment

#	Threat Event	Description	Threat Source	In Scope (Yes/No)	Rationale (if out of scope)
T01	Deliver undirected malware (CAPEC-185)	Thread source delivers malware by providing removable media prepared with malware. Removable media is e.g. left on a parking lot and picked up by hospital staff. USB stick finds its way to the Navigation System. Malware eploits known a known vulnerability and e.g. gains admin priviledges. Undirected attack on computer systems.	TSA-3 - Skript Kiddies	Yes	n/a
T02	Deliver directed malware (CAPEC-185)	Thread source delivers malware on a removable media which was designed to exploit a known vulnerability of the Navigation System. Directed attack on the Navigation System using knowledge about the Navigation System.	TSA-2 Organization	Yes	n/a
T03	Gaining Access ([S]TRID[E])	This phase is where an attacker breaks into the system/network using various tools or methods. After entering into a system, he has to increase his privilege to administrator level so he can install an application he needs or modify data or hide data	TSA-2 Organization	Yes	n/a
T04	Maintaining Access (TTP)	The aim is to maintain the access to the target until he finishes the tasks he planned to accomplish in that target.	TSA-2 Organization	Yes	n/a
T05	Clearing Track (TTP)	This involves modifying/corrupting/deleting the values of Logs, modifying registry values and uninstalling all applications he used and deleting all folders he created	TSA-2 Organization	Yes	n/a
T06	Elevation of privilege (STRID[E])	Identify weaknesses of segregation in terms of administrative and user-level privileges	TSA-2 Organization	Yes	n/a
T07	Denial of service (STRI(D)E)	Find ways to exhaust or drown out legitimate requests	TSA-3 - Skript Kiddies	Yes	n/a
T08	Information disclosure (STR(I)DE)	Fuzz application parameters or arguments to impact application error disclosures. Identify open ports with their respective services. Incite confidentiality and integrity in the browser interface. Identify clear text communications. Review usage of HTTP headers and user-agent profile. Pinpoint usages of API endpoints and application backend technologies.	TSA-2 Organization	Yes	n/a
T09	Data Access (STR[I]DE)	Access user and application data e.g. by a malicious application or script	TSA-3 - Skript Kiddies	Yes	n/a
T10	Open network port exploit (TTP)	Penetrate Open and Unsecured Ports	TSA-3 - Skript Kiddies	Yes	n/a
T11	Brute-force Attack (CAPEC-112)	The brute-force attack contained a dictionary of well-known directories and authentication paradigms present in common webservers.	TSA-2 Organization	Yes	n/a
	Social Engineering (TTP)	create custom phishing scams, phone-based attacks and ev	TSA-3 - Skript Kiddies	Yes	n/a
T13	Lack of evidence to conclude any malicious attempt/attack (ST[R]IDE)	All the actions/events should be properly logged and the content needs to be protected by proper access rights.	TSA-2 Organization	Yes	n/a
Т14	Unauthorized Alterations (S[T]RIDE)	This involves modifying registry values, deleting/encrypting Confidential info and uninstalling Any secure applications and renaming/deleting all files/folders	TSA-2 Organization	Yes	n/a

Printed copies for reference only

Stryker Confidential - This document contains information that is confidential and proprietary. Neither this document nor the information herein may be reproduced, used, or disclosed to or for the benefit of any third party without the prior written consent of Stryker.

Stryker Confidential Page 4 of 29

Form

Research An Form Security Risk Assessment																				
Adverse Impact	ality (N			Pre-impi	elementation of Security Controls					Security Controls/Mitigations		hill b				Post-Implen	nentation of Security Cont	rols		
ID # Threat Event(s) Vulnerabilities Asset Impact Description	Safety Impact (Risk ID# or N/A)	Attack Vector Attack Complexity	Privileges Required User Interaction	Scope Exploit	itability Sub Score ISC Base Impact Sub Score	CVSS v3.0 Base Score	Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score	Risk Security Risk Control Measures Implementation of Risk Control Measures	ol Verification of Risk Control Measures (Effectiveness)	Confidentia Integrity Availability	Attack Vector	Attack Privileg omplexity Require	ges User ed Interaction	Scope	Score ISC Bas	e Impact Sub CV: Score Base	S v3.0 Overall Risk Score Score	Security Rick Level Residual Security Risk Acceptability Justification SOM Reference
1 (Bulliors undirected malaure (LaPEC-185) (Unprotected external UEB Port and the tablet/devices. Tablet Resources—who cam, and Additions unification of computer resources (Resource) (SIS, Tablet and Computer (SIS, T	NA NA									Asset should be behind stateful firewall Anti-virus with updated virus definitions Detection/Protection	Penetration Testing Protocol Document #: D001020037 Security Penetration Test Report: D001020164									Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk. [Red.] High Risk (red) region or in the Medium
Application, Network interfaces: 4) ransonoware attack (Blustooth, Wifi) 5] Bircoin mining, etc										Audit/System log capturing any abnormal activity identified/reported by the application the hardened interfaces (n/w) & anti-mahware mechanism	Report: D001020164 f DSTC001: GSL-STC-01									Rose (yearow) region. However, the individual risks were evaluated and reduced to AFAP to crosses the controls and
T01 V23 A01	Low Low Low	Physical Low	Low Required	Unchanged	0.5 0.5 3.4	3.9	Low	0.20	3.5	LOW secure tunnel communications channel Application shall have logs of table applica	t	Low Low Low	Physical	Low Low	Required	Unchanged	0.5 0.5	3.4	3.9 3.5	LOW mitigations are adequately established to reduce the overall risks to the As far as Possible Levels.
										4. SRS D001020024 -2.17.2The Application shall provide socure										
2 Deliver undirected malware (LAPEC-185) Unprotected external USB Port on the tablet/ devices. System Component 2) computing power 3) devided services and the tablet of the component 3) devided service attacks,	NA									LOW 1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions Detection/Protection	Penetration Testing Protocol Document #: D001020037 Security Penetration Test									Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red.) High Risk (red) region or in the Medium
4) ransomware attack T01 V23 A03 5) Bitcoin mining, etc	Low Low Low	Physical Low	Low Required	Unchanged	0.5 0.5 3.4	3.9	Low	0.2	3.5	3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) &	Report D001020164 DSTC001: GSL-STC-02	Low Low Low	Physical	Low Low	Required	Unchanged	0.5 0.5	3.4	3.9 3.5	Risk (yellow) region. LOW However, the individual risks were evaluated
										secure tunnel communications channel										and reduced to AFAF to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible Levels.
3 Delever undirected malware (CAPEC-18S) External communications and exposure for communication of computer resources exposure for communication (Animels from and to application) System Component (3) defined of writer attacks, and device like habit and and exposure like habit and an exposure attacks (4) connounces attacks.	NA .									LOW 1. Asset should be behind stateful firewall 1. SOM D001020115 - 13. Malware 2. Anti-virus with updated virus definitions 3. Audit/System for conturing any 2.3.4. SRS D001020025	Penetration Testing Protocol Document #: D001020037 Security Penetration Test Report D001020164									Risks is broady acceptable since SmartMedic SOM D001020115 - 13. Malware does not have residual risks in the Critical Risk: Detection/Protection (Red) High Risk (red) region or in the Medium Risk (yollow) region.
and devices like stables and 4) consommers attack Vol smartmodic devices. Add 5) illicoin mining, etc	Low Low Low	Network Low	Low Required	Unchanged	2.1 0.5 3.4	5.5	Low	0.2	3.8	abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	DSTC001: GSL-STC-03	Low Low Low	Network	Low Low	Required	Unchanged	2.1 0.5	3.4	5.5 3.8	LOW However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitiations are adocusted vestibilities to
Deliver undirected malware (CAPEC-185) exposure for communications and exposure for communications microphone, OTG devices, 2) computing power Indication utilization of computer resources microphone, OTG devices, 2) computing power Indication utilization of computer resources microphone, OTG devices, 2) computing power Indication utilization of computer resources microphone, OTG devices, 2) computing power Indication utilization of computer resources microphone, OTG devices, 2) computing power Indication utilization of computer resources microphone, OTG devices, 2) computing power Indication utilization of computer resources microphone, OTG devices, 2) computing power Indication utilization of computer resources microphone, OTG devices, 2) computing power Indication utilization of computer resources microphone, OTG devices, 2) computing power Indication utilization of computer resources microphone, OTG devices, 2) computing power Indication utilization of computer resources microphone, OTG devices, 2) computing power Indication utilization of computer resources microphone, OTG devices, 2) computing power Indication utilization of computer resources microphone, OTG devices, 2) computing power Indication utilization of computer resources microphone, OTG devices, 2) computer Indication utilization of computer resources microphone, OTG devices, 2) computer Indication utilization utilizat	NA NA									LOW 1. Asset should be behind stateful firewall 1. SOM D001020115 - 13. Malwara	Penetration Testing Protocol		-							reduce the overall risks to the As far as Possible Levels. Risk is broady acceptable since SmartMedic SOM D001020115 - 13. Malware
(CAPEC-18ES) evapourse for communications microphone, OTG devices, Temporal Computing grover for communications and obseplications and devices like stablet and page-lacation surveys to the control of the communication o										2. Anti-virus with updated virus definitions 3. Andit/System log capturing any shormal activity identified/reported by Application shall support the use o	Document #: D001020037 Security Penetration Test Report: D001020164									does not have residual risks in the Critical Risk. [Red.] High Risk [red] region or in the Medium Risk (yellow) region.
T01 V22 A01	Low Low Low	Network Low	Low Required	Unchanged	2.1 0.5 3.4	5.5	Low	0.2	3.8	the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel 3.SRS D001020024-2-23.1 The	DSTC001: GSL-STC-04	Low Low Low	Network	Low Low	Required	Unchanged	2.1 0.5	3.4	5.5 3.8	However, the individual risks were evaluated and reduced to ARP to ensure the controls and and reduced to ARP to ensure the controls and mitigations are adequately established to reduce the overtal risks to the Art are Possible for the control of the ARP and the ARP are possible for the control of the ARP and the ARP are possible for the ARP and the ARP are possible for the ARP and the ARP are possible for the ARP and the ARP and the ARP and the ARP are possible for the
										Application shall have logs of table application and firmware (SmartMedic devices).	d.									reduce the overall risks to the As far as Possinee Levels.
Deliver undirected malware Legacy system identification if Smart medic (Stryker device) 1) Mulicious utilization of computer resources	NΔ									4. SRS D001020024-2.17.2The Application shall provide secure tunnel Communications channel LOW 1. Asset should be behind stateful forward 1. SVM D00102015.13 Molyaco	Penetration Testing Protocol									Risk is broady acceptable since SmartMedic SOM D001020115 - 13. Malware
(CAPEC-185) any System Component 2] computing power 3] denial of service attacks, 4 ransonwar attack										Anti-virus with updated virus definitions Audit/System log capturing any 2,3,4. SRS D001020025	Document #: D001020037 Security Penetration Test Report: D001020164									does not have residual risks in the Critical Risk Detection/Protection (Red), High Risk (red) region or in the Medium Risk (rellow) region.
T01 V22 A83 5 Bitcoin mining, etc	Low Low Low	Physical Low	Low None	Unchanged	0.7 0.5 3.4	41	Low	0.2	3.6	abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	DSTC001: GSL-STC-05	Low Low Low	Physical	Low Low	None	Unchanged	0.7 0.5	3.4	4.1 3.6	and reduced to AFP to ensure the controls and mitigations are afecuately established to
6 Deliver undirected malware (CAPEC-185) Lagacy system identification if Tablet Resources - web cam, microphone, OTG-devices, 2] computing power any Lagacy system identification if microphone, OTG-devices, 2] computing power	NA NA									LOW 1. Asset should be behind stateful firewall 1. SOM D001020115 - 13. Malware 2. Anti-virus with updated virus Detection/Protection	Penetration Testing Protocol Document #: D001020037									reduce the overall risks to the As far as Possible Lexek. Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk. Underson have residual risks in the Critical Risk.
(CAPEC-185) any microphene, O'T-Gericce, Removable USI, Table Application, Network interfaces ((Bustenda, WG) 5) Removable using the 6) Re										definitions 3. Audit/System log capturing any abnormal activity identified/reported by Application shall support the use o	Security Penetration Test Report: D001020164									(Red). High Risk (red) region or in the Medium Risk (yellow) region.
T01 V22 A01	Low Low Low	Physical Low	Low None	Unchanged	0.7 0.5 3.4	41	Low	0.2	3.6	Use hardened interfaces (n/w) & secure tunnel communications channel 3 SRS 00010200742 73 1 The		Low Low Low	Physical	Low Low	None	Unchanged	0.7 0.5	3.4	4.1 3.6	However, the individual risks were evaluated and reduced to AFAP to enterior the controls and militigations are adequately established to reduce the overall risks to the As far as Possible Levels.
										Application shall have logs of table application and firmware (SmartMedic devices) 4. SRS D001020024-2-17.2The										Levek.
7 Deliver undirected malware [Inflictive patch management of Device Maintainence tool [QLPEC-185] Device Maintainence tool [Inflictive patch management of QLPEC-185] [Purpose of Computer resources [Uniform Computer resources [Uniform Computer resources [Uniform Computer resources of Computer resources of Computer resources [Uniform Computer resources of Computer resources	NA NA									Application shall provide secure tunnel Communications channel LOW 1. Asset should be behind stateful firewall Device maintainence tool not	Penetration Testing Protocol									Risk is broady acceptable since SmartMedic
(CAPEC-185) [fervare, OS and applications thoughput to information prover 13 denial of writer attack; system plan (your plan plan of the order of th	Low Low Low	Local Low	Low Nome	Unchanged	1.8 0.5 3.4		Low	0.2	3.8	2. Anti-virus with updated virus definitions. 3. Andit/System log capturing any abnormal activity identified/reported by	Security Penetration Test Report: D001020164	Low Low Low	Local	Low Low	None	Unchanged	1.8 0.5	24	5.3 3.8	does not have residual risks in the Critical Risk (Red.) High Sak (red) region or in the Medium Risk (yellow) region.
	LOW LOW LOW	LUCAL LUCA	10000	Una managera						the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	DSTC001: GSL-STC-07	Dir Dir		2011	1000	Oil Indiana				However, the individual risks were evaluated and reduced to ARP to ensure the controls and mitigations are adequately established to reduce the overall relicts to the AR are Possible
8 Obliver undirected malware (CAPEC-185) Interfective patch management of (CAPEC-185) Training to the complete the complete training tr	NA NA									LOW 1. Asset should be behind stateful firewall 2. Anti-virus with updated virus Detection/Protection	Penetration Testing Protocol Document #: D001020037									Risk is broady acceptable since SmartMedic SOM D001020115 - 13. Malware does not have residual risks in the Critical Risk Datection/Protection
(EAPEC 185) (fewer, CS and applications enicephone, OTC devices, English (Februaries) (Februarie										definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application the application 2. SRS D001020024-2.17.6The Application shall support the use o anti-malware mechanism	Security Penetration Test Report: D001020164 f DSTC001: GSL-STC-08									[Red.] High Risk (red.) region or in the Medium Risk (vylloow) region. However, the risks were evaluated
T01 V08 A01	Low Low Low	Local Low	Low None	Unchanged	1.8 0.5 3.4	53	Low	0.2	3.8	4. Use hardened interfaces (e/w) & secure tunnel communications channel as SSS 5001020024-2-23.1 The Application and firmsare (SmartMedic devices).	t	Low Low Low	Local	Low Low	None	Unchanged	1.8 0.5	3.4	5.3 3.8	and reduced to AFAP to ensure the controls and mitigations are adequately exhibition to reduce the overall risks to the As far as Possible
										4. SRS D001020024 -2.17.2The										1000
9 Deliver undirected malware (CAPEC-18S) firware, CS and applications System Component 2 computer resources (System Component 2) computing power	NA NA									Application shall provide secure tomos! Communication; channel Low 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malware 2. Anti-virus with updated virus 5. Detection/Protection	Penetration Testing Protocol Document #: D001020037									Risk is broady acceptable since SmartMedic does not have residual risks in the Crisical Risk. Detection/Protection
thoughout the information system plan 33 denial of service attack; 41 ransonmeures 45 particular Add 51 Bitcoin mining, etc	Low Low Low	Local Low	Low None	Unchanged	1.8 0.5 3.4	53	Low	0.2	3.8	definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 2,3,4. SRS D001020025	Security Penetration Test Report: D001020164 DSTC001: GSL-STC-09	Low Low Low	Local	Low Low	None	Unchanged	1.8 0.5	3.4	5.3 3.8	(Red). High Risk (red) region or in the Medium Risk (yellow) region.
										Use hardened interfaces (n/w) & secure tunnel communications channel	2010002. 022010-07									and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
10 Deliver undirected malware (CAPEC-185) Device Maintainence tool (Marchaery Software Valencehility (Bardware/Software) J (Maniel of service articles, Management J (Marchaery Software) (Marchaery Software) J (Maniel of service articles, Management J (Marchaery Software) J (Marchaery Software) J (Marchaery Software)	NA									LOW 1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions glasform.	Security Penetration Test									Leveys. Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red.) High Risk (red) region or in the Medium
Management 33 definit of service attacks, 4) amounts attacks, 4) amounts attacks, 5) Bitcoin mining, etc. 100 10	Low Low Low	Local Low	Low None	Unchanged	1.8 0.5 3.4	53	Low	0.2	3.8	Audit/System log capturing any shenormal activity identified/reported by the application Use hardened interfaces (n/w) &	Report D001020164 DSTC001: GSL-STC-10	Low Low Low	Local	Low Low	None	Unchanged	1.8 0.5	3.4	53 38	Risk (yellow) region. LOW However, the individual risks were evaluated and other than the control and the control of the control and the control of the con
										secure tunnel communications channel										mitigations are adequately established to reduce the overall risks to the As far as Possible Levels. Risks be nowledge acceptable since Smarthfeld: SOM D001020115 - 13. Malvare
11 Obliver undirected indusers (LAFEC 1815) CAPEC 1815)	NA									Anti-virus with updated virus definitions Audit/System log capturing any SRS D001020024-2-17.6The	Document #: D001020037 Security Penetration Test Report: D001020164									Risks is broadly acceptables annot SmartMedic does not have residual risks in the Critical Risk (Red.) High Risk (red) region or in the Medium Risk (rellow) region.
(Bluetooth, Wilf) 5) Bizcoin mining, etc	Low Low Low	Local Low	Low None	Unchanged	1.8 0.5 3.4	53	Low	0.2	3.8	abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel 3.SRS D001020024-2.23.1 The	DSTC001: GSL-STC-11	Low Low Low	Lecal	Low Low	None	Unchanged	1.8 0.5	3.4	5.3 3.8	However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to
										Application shall have logs of table application and firmware (SmartMedic devices).	t									LOW mitigations are adequately established to reduce the overall risks to the As far as Possible Levels.
										4. SRS D001020024 - 2.17.2The Application shall provide secure bonned Tammunications channel LOW 1. Asset should be behind stateful firewall 1. SOM D001020115 - 13. Mahouri	Penetration Testing Protocol									
12 Deliver undirected malware (CAPEC-185) Software Veherability Mainagement System Component 5) Bencin mining, etc. 1) Bencin mining, etc.	ting power NA									2. Anti-virus with updated virus definitions 3. Audit/System log capturing any 2,3,4. SRS D001020025	Document #: D001020037 Security Penetration Test Report: D001020164									Rick is broady acceptable since SmartMedic. does not have recipital ricks in the Critical Rock. (Red.) High Rick (red.) region or in the Medium Rick (pelloy) Figure.
T01 V09 A83	Low Low Low	Local Low	Low None	Unchanged	1.8 0.5 3.4	53	Low	0.2	3.8	abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	DSTC001: GSL-STC-12	Low Low Low	Local	Low Low	None	Unchanged	1.8 0.5	3.4	5.3 3.8	However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to
13 Deliver audiocede natureus Uniprotected auteurs period in (APTC-181) Deliver audiocede natureus period computer resources points points (APTC-181) Deliver audiocede natureus period (APTC-181) Deliver audiocede natureus period (APTC-181) Deliver audiocede natureus (APTC-181) Deliver audiocede	NA NA									LOW 1. Asset should be behind stateful firewall 1. SOM D001020115 - 13. Malware 2. Anti-virus with updated virus Detection/Protection	Penetration Testing Protocol Document #: D001020037									minigitation are analoquiatory extensioned to reduce the overall first to the Ast far as Possible towards Risk is broadly acceptable since SmartMedic SoM D001020115 - 13. Malware does not have residual risks in the Critical Risk Detection/Protection
13 Offerer audirected authorizes (LAPEC-1815) (Impaire desirements profit) on the content of computer resources (LAPEC-1815) (Impaire desirements devices and connections paints) (Impaire desirements devices and connections paints) (Impaire devices and connections paints) (Impaire devices and connections paints) (Impaire devices and connections) (Impaired dev										definitions 3. Audit/System log capturing any abnormal activity identified/reported by Application shall support the use o	Security Penetration Test Report: D001020164									does not have residual risks in the Critical Risk. (Red.) High Risk (red) region or in the Medium Risk (rellow) region. However, the institutual risks were evaluated.
T01 V12 A01	None None High	Network Low	High None	Unchanged	1.2 0.6 3.6	49	Low	0.2	3.9	the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel 3.585 D001020024-2.23.1 The	DSTC001: GSL-STC-13	None None Low	Network	Low High	None	Unchanged	12 02	1.4	27 1.7	and reduced to ASAR to ensure the controls and
										Application shall have logs of table application and firmaces (SmartMedic devices). 4. SRS D001020024-2.17.2The										Lovols.
14 Deliver undirected malware (CAPEC-185) Improving a form of the connection of computer resources (CAPEC-185) Indictions utilization of computer resources (System Component 2) computing power 2) computing power	NA NA									Application shall provide secure function of the secure shall provide secure function of the secure shall 1. SOM D001020115-13. Malwara LOW 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malwara LOW 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malwara LOW 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malwara LOW 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malwara LOW 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malwara LOW 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malwara LOW 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malwara LOW 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malwara LOW 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malwara LOW 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malwara LOW 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malwara LOW 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malwara LOW 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malwara LOW 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malwara LOW 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malwara LOW 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malwara LOW 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malwara LOW 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malwara LOW 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malwara LOW 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malwara LOW 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malwara LOW 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malwara LOW 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malwara LOW 1. Asset should be behind stateful firewall 1. SOM D001020115-13. Malwara LOW 1. Asse	Penetration Testing Protocol									Risk is broady acceptable since SmartMedic SOM D001020115 - 13. Malware
(CAPEC-185) answord devices and connection points points you and connection points you are connected and connection points you are connected and connection points you are connected and points you are connected a										2. Anti-virus with updated virus definitions 3. Audit/System log capturing any shoormal activity identified/reported by	Document #: D001020037 Security Penetration Test Report: D001020164			.					.	does one have residual risks in the Critical Risk (Red.) High Risk (red) region or in the Medium Risk (yellow) region.
100	None None High	Network Low	High None	Unchanged	1.2 0.6 3.6	49	Low	0.2	3.9	the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	DSTC001: GSL-STC-14	None None Low	Network	Low High	None	Unchanged	1.2 0.2	1.4	2.7 1.7	LOW However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately exhibited to reduce the overall risks to the ket far as Possible
15 Deliver undirected malware (LAPEC-185) Description (LAPEC-185)	NA NA									LOW 1. Asset should be behind stateful firewall 2. Anti-virus with updated virus Detection/Protection	Document #: D001020037									Feducie The oversalt risks to the As List as Possante Levols. Risk is brandy acceptable since SmartMedic does not have residual risks in the Critical Risk (Red) Righ Risk (red) region or in the Medium
15 Onliver undirected malware (LAPEC-185) Table Resources:										definitions 3. Audit/System log capturing any abnormal activity identified/reported by Application shall support the use of	Security Penetration Test Report: D001020164									Risk (yellow) region. However, the individual risks were evaluated
T01 V16 A01	Low Low Low	Local Low	Low None	Unchanged	1.8 0.5 3.4	53	Low	0.2	3.8	Use hardened interfaces (n/w) & secure tunnel communications channel 3 SRS 00010200742 73 1 The		Low Low Low	Local	Low Low	None	Unchanged	1.8 0.5	3.4	5.3 3.8	
										Application shall have logs of table application and firmours (SamatMedic devices). 4. SRS D001020024-2.17.2The										
16 Deliver undirected malware [Unencypted data in transit in all Smart mode(Stysher device) 1] Multicious utilization of computer resources [CLPEC-185] Bowchamels System Component 2] computing goover	NA NA									Application shall provide secure toward 1. Asset should be behind stateful firewall 1. Soot of Detection Protection 2. Anti-virus with updated virus 2. Detection/Protection	Penetration Testing Protocol Document #: D001020037									Risk is broady acceptable since SmartMedic does not have residual risks in the Criscal Risk Detection/Protection
33 defaul of wrive attacks, 4) reasonmove attack 4) reasonmove attack 5) Bitcoin mining, etc.	None None High	Network Low	High None	Unchanged	12 06 36	49	Low	0.2	3.9	definitions 3. Audit/System log capturing any abnormal activity identified/reported by	Security Penetration Test Report: D001020164 DSTC001: GSL-STC-16	None None Low	Network	Low High	None	Unchanged	1.2 0.2	1.4	27 17	(Red). High Risk (red) region or in the Medium Risk (yellow) region.
										the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel										Honever, the individual risks we're evaluated and reduced to AFAP to ensure the controls and mitigations are adoptically established to reduce the overall risks to the Ast are Possible
17 Deliver undirected malware (CAPEC-185) (CAPEC-185) (CAPEC-185) (CAPEC-185) (Descripted data in transit in all flowchamels (CAPEC-185) (CAPEC-185) (Descripted data in transit in all flowchamels (CAPEC-185) (CAPEC-185) (Descripted data in transit in all flowchamels (CAPEC-185) (CAPEC-185) (Descripted data in transit in all flowchamels (CAPEC-185) (CAPEC-185) (Descripted data in transit in all flowchamels (CAPEC-185) (CAPEC-185)	NA									LOW 1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions definitions	Document #: D001020037 Security Penetration Test									Risk is broady acceptable since SmartMedic does not have residual risks in the Criscal Risk (Flort) Hard Right front principal or in the Medicine (Flort) Ha
(CAPEC-185) Browchamuch microphone, OTC devices, [2] compring power [3] contained from the filter product (SER Table 1), closed of a review attricks, [3] contained from the filter product (SER table 1), closed (SER table										Audit/System log capturing any abnormal activity identified/reported by the application SSS D001020024-2-17.6The Application shall support the use of anti-malware mechanism.	Report: D001020164									Risk (yellow) region. However, the individual risks were evaluated
T01 V17 A01	None None High	Network Low	High None	Unchanged	12 06 36	49	Low	0.2	3.9	Use hardened interfaces (n/w) & secure tunnel communications channel Assis D001020024-2-23.1 The Application shall have logs of table application and firmware	t	None None Low	Network	Low High	None	Unchanged	1.2 0.2	1.4	27 1.7	and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible Levels.
										(SmartMedic devices). 4. SRS D001020024-2-17.2The Application shall provide secure										
										Apparation stail provide secure tunnel Communications channel										

Stryker Doc Number: D000000999 Name: Product Security Risk Table Revision: AB Form

Threat Event(s)	Vulnerabilities	Asset	Adverse Impact Impact Description	Safety Impact (Risk ID# or N/A)	onfidentiality	Integrity Availability	Attack Vector	Attack Complexit	Privileges Required	User Interaction		Pre-Implementation of Se- Exploitability Sub Score	ISC Base Imp	nact Sub Score	CVSS v3.0 Base Score	Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score	Security Risk Security Risk Control Measur	Implementation of Risk Co Measures	trol Verification of Risk Control Measures (Effectiveness)	onfidentiality Integrity	Attack Vector	Attack Complexity	Privileges U Required Inter-	liser Sc	exploitabilit Score	y Sub 1SC Base	mpact Sub Score Base Sc	3.0 Overall Risk ore Score	Security Risk Residual Security Risk Acceptability Level Justification	Remarks (Colur SOM Reference
or undirected malware EC-185)	Outdated - Software/Hardware	Device Maintainence tool (Hardware/Software)	Malicious utilization of computer resources computing power di denial descrive attacks, 4) ransomware attack Bitcoin mining, etc	NA NA	Low	Low Low	Physical	Low	Law	None	Unchanged	0.7	0.5	3.4	41	Moderate	as	3.8	LOW 1. Assert should be behind stateful of 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/report the application 4. Use hardened interfaces (a/w) 4 secure tunnel communications cha	rewall Device maintainence tool not implemented/existing in the S0 platform. d by	Penetration Testing Protocol Document #: D001020037 Security Penetration Test Report D001020164 DSTC001: GSL-STC-18	Low Low I	Low Physical	Low	Low N	Sone Unc	hanged 0.7	0.5	3.4 4.1	1 3.8	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Ri (Red,) High Risk (religion or in the Medi Risk (yellow) region. LOW However, the individual risks were evaluate and reduced to AFAP to ensure the controls mitigations are adequately established to reduce the overall risks to the Afa as a Post reduce to the reversal risks to the Afa as a Post	tisk ium ed
r undirected malware C-185)	Outdated - Software/Hardware	Smart medic (Stryker device) System Component	Malicious utilization of computer resources Computing prower Solution of service attacks, A ransonmers attack Bitcoin mining, etc	NA	Low	Low Low	Physical	Low	Law	None	Unchanged	0.7	0.5	3.4	41	Moderate	0.5	3.8	Asser should be behind stateful for 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reports peptication 4. Due hardened interfaces (n/w) 4 secure tunnel communications cha	ewall 1. SOM D001020115 - 13. Malw Detection/Protection 2.3,4. SRS D001020025 tol	Penetration Testing Protocol Document #: D001020037 Security Penetration Test Report: D001020164 DSTC001: GSL-STC-19	Low Low I	Low Physical	Low	Low N	None Unc	hanged 0.7	0.5	3.4 4.1	1 38	Leoobi. Risk is broasdy acceptable since SmartMedic does not have residual risks in the Critical Sta (Risk). High Risk (cell regions or in the Model Risk (Walder) region. LOW LOW LOW LOW Mingrand and Control of the Model and reduced to AFAF to ensure the control intigations are adequately established to	SOM D0010201 Detection/Proteinm
ndirected malware (85)	Outdated - Software/Hardware	Tablet Resources - web cam, microphone, O'Tc devices, Removable USR, Tablet Application, Network interface (Blustooth, Wiff)	Nations utilization of computer resources computing power computing review	NA	Low	Low Low	Physical	Low	Low	Nome	Unchanged	0.7	ē.S	3.4	41	Low	82	3.6	Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reporthe application Mo bardened interfaces (n/w/)	twall 1. SOM D001020115 - 13. Malw Detection/Protection 2. SRS D001020024 - 2.17.8The dd by Application shall support the stand-understand shall support the stand-understand shall support the stand-understand shall supplication shall have logs of trapplication shall have logs of trapplication shall have logs of trapplication shall have logs of the standard shall have logs of the standard shall have logs of the	Document #: D001020037 Security Penetration Test Report: D001020164 of DSTC001: GSL-STC-20	Low Low 1	Low Physical	Low	Low N	Sone Unc	hanged 6.7	0.5	34 41	1 36	renders the overall rinks to the Art are Nove Tall is travely acceptable confused from the Medical does not have resistant rinks in the Critical Eq. (Ball). Bigs [Said [red] regions or in the Medical link; (bythos) riginal. However, the individual rinks were evaluate the confused of the Company of the Company of the minigations are adequately established to relate the confused of the Company of the Company of the Company of the Company of the Company of the levels.	SOM D0010201 kisk Detection/Protium ed s and
ected malware 5)	InSecure Configuration for Software/US on Mobile Devices, Laptops, Workstations, and Servers	Device Maintainence tool (Hardware/Software) A05	Malicious utilization of computer resources computing power definition of computer resources definition o	NA	None	None High	Local	Low	High	Required	Unchanged	0.6	0.6	36	42	Moderate	0.50	39	I. Asser thould be behind stateful C Anti-virus with updated virus definitions 3. Audis/System log capturing any abnormal activity identified/report application 4. Use hardened interfaces [a/w] secure tunnel communications cha	Application shall provide secur tunnel Communications channe ewall Device maintainence tool not implemented/existing in the SI platform.	Penetration Testing Protocol Document #: D001020037 Socurity Penetration Test Report: D001020164 DSTC001: GSL-STC-21	None None 1	Low Local	Low	High Req	quired Unc	hanged 0.6	0.2	1.4 2.0) 18	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red.) High Risk (red) region or in the Medis Risk (systlow) region. LOW However, the individual risks were evaluate and reduced to AFAP to ensure the controls mitigations are adoptably established to a single residence are adoptably established to a mitigations are adoptably established to a single residence are adoptably established to a single residence are adoptably established to a single residence are adoptable residence.	isk ium ed i and
ted malware	InSecure Configuration for Software/US on Mobile Devices, Laptops, Workstations, and Servers	Smart medic (Stryker device) System Component	Malicious utilization of computer resources Computing power Sometime of the control	NA	None	None High	Local	Low	High	Required	Unchanged	0.6	0.6	3.6	42	Moderate	a s	3.9	I. Assert should be behind stateful of Anti-virus with updated virus definitions I. Audit/System log capturing any abnormal activity identified/report the application 4. Due hardened interfaces (n/w) a secure tunnel communications cha	ewall 1. SOM D001020115 - 13. Malw Detection/Protection 2,3,4. SRS D001020025 d by	Penetration Testing Protocol Document #: D001020037 Security Penetration Test Report: D001020164 DSTC001: GSL-STC-22	None None I	Low Local	Low	High Req	quired Unc	hanged 0.6	0.2	1.4 2.0	0 18	reduce the overall risks to the As for as Poss. Levels. Risk is breash as copyrated since SmartMedic does not have residued risks in the Critical (Big (Bod.) Flight, Risk (red) regions or in the Media (Vellow) regions. LOW However, the individual risks were evaluate and reduced to ASP or nounce the controls of the content for controls on individual risks were evaluated in the control of the Cont	SOM D0010: Detection/P
ected malware 5)	Inforcuse Gonfiguration for Software/US on Mobile Devices, Lisping, Workstations, and Servers	Tablet Resources - web cam, microphone, OTG devices, Removable USR, Tablet Application, Network interface (Bluetooth, Wiff)	Malicious utilization of computer resources Computing power Social Section (Section 2) Social of service attack Social section mining, etc	NA	Low	Low Low	Local	Low	Low	Required	Unchanged	13	as	3.4	48	Low	02	37	Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reporthe application Mo bardened interfaces (n/w) if	d by Application shall support the us anti-malware mechanism	Document #: D001020037 Security Penetration Test Report: D001020164	Low Low 1	Low Local	Low	Low Req	quired Unc	hanged 1.3	0.5	3.4 4.8	3 37	Figure 1 received from the contract of the con	SOM D00102 bisk burn ed and
ected malware 5)	Unprotected external USB Port on the tablet/devices.	Wireless Network device (Scog of HDO)	e 1) Malicioss utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransonsware attack 5) Becoin mining, etc	NA	Low	Low Low	Physical	Low	Law	Required	Unchanged	0.5	0.5	3.4	39	Moderate	Q S	3.7	LOW SOM responsibility 1. Statefulf Ferewall 2. Maintain access control (read/m permission list for any sensitive & unencrypted data if present.	Application shall provide socur mosel Communications channel 1. SOM DO01020115 - 13 Mails Detection/Protection 2. SOM D001020115 - 7.1. Acus control policy and management	Penetration Testing Protocol Document #: D001020037 Socurity Penetration Test Report: D001020164 DSTC001: GSL-STC-24	Low Low I	Low Physical	Low	Low Req	quired Unc	hanged 0.5	0.5	3.4 39	3.7	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Ric (Red.) High Risk (red) region or in the Medi Risk (redlow) region. LOW However, the individual risks were evaluate and reduced to AFAP to ensure the controls mitigities are an eleganticly established to a mitigities are are designed;	ed and
ected malware	Unprotected enternal USB Port on the tablet/devices.	Tablet Besources - web cam, microphone, OTG devices, Removable USR Tablet Application, Network interface (Bluetooth, Wiff)	Malicious utilization of computer resources Computer power Computer statch,	NA NA	Low	Low Low	Physical	Low	Low	Required	Unchanged	0.5	0.5	34	39	Moderate	āS	37	 Anti-virus with updated virus definitions Audit/System log capturing any 	d by Application shall support the us anti-malware mechanism	Document #: D001020037 Security Penetration Test Report: D001020164 of DSTC001: GSL-STC-25	Low Low 1	Low Physical	Low	Low Req	quired Unc	hanged 0.5	0.5	34 39) 37	reduce the event all risks to the Ast for an Young- Leads. Leads and a complete and a complete and the comp	SOM D0010 lisk Detection/P
ected malware (5)	Unprotected external USB Port on the tablet/devices.	Smart medic app (Stryker Adm Web Application)	in 1) Malicion utilizazion of computer resources 2) computing power 3) donial of survice attack, 4) (restomene attack, 2) intection intellige are	NA NA	Low	Low Low	Physical	Low	Low	Required	Unchanged	øs.	ūS .	3.4	3.9	Low	0.2	15	Lower dound be behind counted Anti-view with updated street Anti-view with updated street Anti-view of distilions Lower of the counter of the counter Lower of the counter of the counter Lower of the counter of the counter Lower of the counter Anti-view of the counter Lower of the counter of the counter Lower of the counter of the counter Lower of the counter of the counter	d by to view the functionality of diffi components existing in the SM platform. Admin app doesnt co	Document #: D001020037 Socurity Penetration Test Beport: D001020164 rest port: D00102016	Lane Lane 1	Low Physical	Low	Low Req	quired Unc	hanged 0.5	a. 5	3.4 3.9	35	Bit is bready acceptable sizes Startfelded does not have residual risks in the Critical II (Ital) IIIsh bits (red propose or in the Media IIIsh (Ital) IIIsh bits (red propose or in the Media IIIsh (red) rejuns. Henever, the individual risks were evaluated and reduced to MAPI to resume the controls and reference to MAPI to resume the controls mitigation are advantaged scalarification for the control risks have been been event risks to be do for an Youn Levels.	lisk Detection/Pr ium ed and
cted malware	External communications and exposure for communication channels from and to application and devices like tablet and martmetic device. VG2	Tablet Recourses - web care, nicrophone, OTC devices, Removable ISR, Tablet Application, Network interface (Illustrooth, Wiff) A01	1) Malicious utilization of computer resources 2) computing power 2) computing power 40 / sametomase at tack 5) Bitcoin mining, etc	NA NA	None	None High	Network:	Low	High	Required	Unchanged	0.9	0.6	3.6	45	Moderate	ēS	41	NESON 1. Only only for made (infraestrate) advices thould communicate with the anested refere for thather 2. Assert should be behind nated if 3. But seems trained communicate distance of the second that is not the second that is	4. SSS. D00120907 - 2.17 5The Application shall provide secure trained Communications chains and the communication of the control provides and tables. 1. SSE D00020012 - 2.7 1-8. Only should be able to communication in the communication of the communication of the secure training of the communication of the communication of the perfect of the communication of the communication of the communication of the communication of the communications chains	ly Penetration Testing Protocol Sociates Document #: D001020037 Sociatify Penetration Test Report: D001020164 DSTC001: GSL-STC-27	None None I	Low Network	Low	High Req	quired Unc	hanged 0.9	0.2	1.4 2.4	19	Ball is broady acceptable sizes SnartMedic does not have readed rich in the Crist of the Crist of the Crist of the Crist of the Ball (Spring) region. However, the indicator rich were evaluated and readed to MAFF to resum the Crist of the miligations are adequately architected to the control of the Crist of the Crist of the Crist levels.	lisk Detection/F ium ed s and
ected malware 5)	Ineffective patch management of firware, OS and applications thoughout the information system plan V08	Device Maintainence tool (Hardware/Software) A05	Malicious utilization of computer resources Computing power Somital of service attacks, A ransonmers attack Bitcoin mining, etc	NA NA	Low	Low Low	Local	Low	Law	None	Unchanged	1.8	0.5	3.4	53	Low	02	3.8	I. Asset should be behind stateful fi 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any absormal activity identified/report the application 4. Use hardened interfaces (n/w) 8 secure tunnel communications cha		Penetration Testing Protocol Document #: D001020037 Security Penetration Test Report: D001020164 DSTC001: GSL-STC-28	Low Low 1	Low Local	Low	Low N	None Uncident	hanged 1.8	0.5	3.4 5.3	3.8	Risk in broady acceptable since SmartMedic does not have residual risks in the Critical Richell (Bod) High Rosi (red) regions or in the Medic Richell Richell (Rosi) Rosi (red) regions or in the Medic Richell Richel	ed and
cted malware	Ineffective patch management of firware, OS and applications thoughout the information system plan	Smart medic (Stryker device) System Component	3) Malicious utilization of computer resources 2) computing prover 3) denial of service attacks, 4) ransonswer attack 5) Bitcoin mining, etc	NA	Low	Low Low	Local	Low	Low	None	Unchanged	1.8	a 5	3.4	53	Low	02	38	1. Asser should be behind stateful of 2. Anti-virus with updated virus definitions 3. Andi-virus with updated virus definitions 3. Andi-virus with updated virus shootmal activity identified/report he application 4. Die hardened interfaces (n/w) & secure tunnel communications cha		Penetration Testing Protocol Document #: D001020037 Security Penetration Test Report: D001020164 DSTC001: GSL-STC-29	Low Low 1	Low Local	Low	Low N	Sone Unc	hanged 1.8	0.5	3.4 5.3	3 3.8	Levols Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Ri (Red). High Risk (red) region or in the Medic Risk (vellow) region.	SOM D0010 Clisk Detection/F ium
cted malware	Intellective patch management of fivewer, OS and applications thoughout, OS and applications thoughout the information system plan	Tablet Resources - web cam, microphone, OTC devices, Removable ISR, Tablet Application, Network interface (Biustooth, Wiff) A01	1) Malicious utilization of computer resources 2) computing power 3) denial of nervico articles, 4) prantomore article 5) Bitcoin mining, etc	NA	Low	Low Low	Local	Low	Low	None	Unchanged	18	0.5	34	53	Low	02	38	 Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/report the application Use hardened interfaces (n/w) it 	d by Application shall support the use and malware mechanism and application shall have logs of usphication and firmware (SmartMedic devices). 4. SRS D001020024 - 2.17.2The	Document #: D001020037 Security Penetration Test Report: D001020164 of DSTC001: GSL-STC-30	Loos Loos 1	Low Local	Low	Low N	Sone Unc	hanged 1.8	0.5	3.4 \$3	38	Levok: Risk is broady acceptable since SmartMedic does not have residual risks in the Critical R (Red). High Risk (red) region or in the Medic Risk (yellow) region. Honever, the individual risks were evaluate and solen ALS Res in the controls.	SOM D0010 bisk Detection/F
ected malware 5)	Unprotected network port(s) on network devices and connection points		Malicious utilization of computer resources computing power So demand of service attacks, demand of service attack So Bitcoin mining, etc	NA NA	None	None High	Network	Low	High	None	Unchanged	12	0.6	36	49	Moderate	āS	43	MEDIUM 1. Only Stryker/HDO authenticated devices should communicate with medic device is tablet. 2. Asset should be behind stateful f. 3. Use secure tunnel communicatio channel	Application shall provide secur tunnel Communications channe 1. SRS D001020025 nart 2. SOM D001020115 - 13. Malw ewall Detection/Protection		None None I	Low Network	Low	High N	Sone Unc	hanged 1.2	0.2	1.4 2.7	7 2.1	Eick is broadly acceptable since SmartMedic does not have residual risks in the Critical Ric (Red.) High Rick (red) region or in the Medic Rick (yellow) region. LOW However, the individual ricks were evaluate and reduced to ARP the resumes the controls endeated to ARP the resumes the controls entirely established to reduce the overall ricks to the Asf as a Food reduced to ARP to the Asf as a Food reduced to ARP to the Asf as a Food reduced to ARP to the Asf as a Food reduced to ARP to the Asf as a Food reduced to ARP to the Asf as a Food reduced to ARP to	tisk Detection/P ium ed a and
cted malware	Unprosected network part[c] on network devices and connection points	Tablet Resources - web cam, microphone, OTG devices, Removable USE, Tablet ARA-GRAND CONTROL (Riserrate Visit Interface (Riserceth, Wiff)	[1] Milicious utilization of computer resources [2] computing power [3] denial of arrivor attacks, [4] reasonmer attack [5] Bitcoin mining, etc.	NA.	None	None High	Network	Low	High	Nome	Unchanged	12	0.6	3.6	49	Low	62	39	Low L. Asser though the behind stanfalf of the Asser through the supplied virus definitions to the control of t	d by Application shall support the use anti-malware mechanism net a SSRS D001020024 - 2-23.1 The Application shall have logs of use application and firmware (SmartMedic devices). 4. SRS D001020024 - 21.7.2The Application shall provide security application shall provide security application shall provide security.	Document #: D001020037 Socurity Penetration Test Report D001020164 of DSTC001: GSL-STC-32	None None I	Low Network	Low	High N	None Und	hanged 12	0.2	1.4 2.7	7 1.7	Levels. Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Rick (Red) Right Risk (red) regions or in the Medic Risk (pollow) regions or the Medic Risk (pollow) regions. However, the individual risks were evaluate and ordered in ARAP to ensure the controls.	SOM D0010 lisk Detection/F
ected malware 5)	InSocure Configuration for Software (US on Mobile Devices, Laptops, Workstations, and Servers	Smart medic app (Stryker Adm Web Application)	in 1) Milliclose utilization of computer resources 2) computing power 3) domind of arrivor attacks, 4) reasonsware attack 5) Becoin mining, etc	NA.	None	None High	Local	High	High	Required	Unchanged	03	0.6	3.6	40	Moderate	e s	38	1. Deployed (VMV) secure system configuration model needs to be meetined in the intallization manu. 2. Establish internal and external admiration sources for first admiration sources for first distance of the configuration sources for first distance of the configuration sources for first distance of the configuration sources for first distance distance of the configuration sources for biglip-priority items. 3. the upgraded software, firms are sourced to the configuration of the configur	numed L'ommunications: channe 1. Using web app the admin can to view the functionality of diff. components existing in the SM platform. Admin app doesnt co any of the system components: the risk associated to the SM pl with admin web app can be ign 2. SOM D001020115-13. Malv Detection/Frotection 3.8SS 10001020195-2.1.7.2.	bble Penetration Testing Protocol Document #: D00120037 Security Penetration Test Report: D001020164 Sence DSTC001: GSL-STC-34 GERMAN CONTROL OF THE PROTOCOL OF THE PENETRAL	None None I	Low Local	High	High Req	quired Unc	hanged 0.3	0.2	1.4 1.8	16	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical EL (EL) (El) (El) (El) (El) (El) (El) (El) (El	lisk Detection/F ium ed and

Stryker Doc Number: D000000999 Name: Product Security Risk Table Revision: AB

Revision: AB Form																														
ID # Threat Event(s)	Vulnerabilities	Asset	Adverse Impact Impact Description	Safety Impact (Risk ID# or N/A)	Integrity Availability	Attack Vector	Attack Complexity	Privileges Required	User Interaction		mplementation of Security Continuous ploitability Sub Score ISC Bi	rols Impact Sub Score	CVSS v3.0 Base Score	Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score	Security Risk Level Security Risk Control Measures	Security Controls/Mitigations Implementation of Risk Control Measures	verification of Risk Control Measures (Effectiveness)	onfide miality Integrify	Attack Vector	Attack Priv Complexity Requ	ileges User nired Interaction		mentation of Security sploitability Sub Score		CVSS v3.0 Or Base Score	verall Risk Security Score Leve	Risk Residual Security Risk Acceptability Remarks (Justification SOM Refer	{ Column added additionaly for rence
34 Deliver directed malware (CAPEC-185) T02	InSecure Configuration for Software/US on Mobile Devices, Laptops, Worksations, and Servers	Tablet Resources - web cam, microphone, OTG devices, Removable USR Tablet Application, Network interfaces (Bluetooth, Wift)	3) Malificion utilization of computer resources 2) ciencipiding person 3) denial of service attack 4) ransomorare attack 5) Blecoin mining, etc	NA Low	e Low Low	r Local	Low	Low	Required I	Inchanged	13 05	3.4	48	Low	02	3.7	Anti-virus with updated virus definitions Audit/System log capturing any	wall 1.50M D001020115-13. Malwar Detection/Protection 2.58S D00102024-2.17.6The Application shall support the use can and-malware mechanism 3.58S D00102024-2.23.1 The Application shall have logs of table application and firmware (SmartMedic devices).	Document #: D001020037 Security Penetration Test Report: D001020164 if DSTC001: GSL-STC-35	Low Low	Low Local	Low 1	ow Required	Unchanged	13	0.5 3.4	4.8	3.7 LOV	Rich is haven by receptable direc Smartheric flowers between board mides in the Confident Confidence flowers between the confidence and the Confidence like (Seedles) regions or in the Medium Rich (profiles) regions or in the Medium Rich (profiles) regions are in the Medium and reduced to ARA'D to connect the controls and miligations are adequately established to reduce the overall richs to the Ast far as Possible Levels.)20115 - 13. Malware Protection
Deliver directed malware (CAPEC-185) T02	Unescrypted data at rest in all possible locations V26	Table Besources - web cam, microphone, OTG devices, Removable USB, Tabler Application, Nework interfaces (Bluetooth, Wiff)	1) Malicions utilization of computer resources 2) computing gover 3) denial of service attacks, 3) denial of service attacks, 5) illication unining, etc	NA Law	e Low Low	r Local	Low	Low	None 1	Inchanged	1.8 8.5	34	53	Low	6.29	18	Anti-virus with updated virus definitions Audit/System log capturing any	4. SSS 10001020024 - 1.17.The Application Studing provide secure Unit 100 to 10	Document #: D001020037 Security Penetration Test Report D001020164 of DSTC001: GSL-STC-36	Low Low	Low Local	Low I	.ow None	Unchanged	18	0.5 2.4	53	3.8 LOV	Bith is broadly acceptable since SmartMedic does not have residual risks in the Chilical Bidd Delect (July 100), play 100 per some in the Medium bids by giving years or in the Medium Bidd Spiritary process of the Spiritary Spiritary 100 per some or evaluated Bidd Spiritary 100 per	J20115 - 13. Malware Protection
26 Deliver directed malware (CAPEC-185) T02	Unencrypted data at rest in all possible locations V16	Tablet OS/notwork details & Tablet Application	Malicious utilization of computer resources 21 computing power 31 denial of warvice statck, 41 yearsonware attack 51 Brecein mining, etc	NA Low	s Love Love	r Local	Low	Low	Nome 1	Inchanged	1.8 0.5	3.4	5.3	Low	0.2	18	Loss Land thould be behind standed for 2. Acts view with pupilated view definitions definitions 3. Audin/Tyram log capturing any the application control of the standard pupilated for the pupi	mnnel Communications channel all 1500 MODIUST 15. 18 Malwaru Detection/Protection Detection/Protection Detection/Protection Detection/Protection Detection/Protection USS ST 0001020024 - 217.5The and malware mechanism il 3.585 D001020024 - 227.1The Application shall have logs of table application and firmware (SmartHedric devices) 4.585 D001020024 - 217.2The	Security Penetration Test Report: D001020164 if DSTC001: GSL-STC-37	Low Low	Low Local	Low I	.ow None	Unchanged	18	0.5 3.4	5.3	3.8 Lov	Risk is brously acceptable since Searchfeder [Red.9] sligh link (red.) region or in the Medium like (red.) sligh link (red.) region or in the Medium like (red.) red. red. like (red.) red. red. like (red.)	320115 - 13. Malware Protection
37 Deliver directed malware (CAPEC-185) T02	Unencrypted data at rest in all possible locations V26	Smart medic app (Stryker Admir Web Application)	Mulicious utilization of computer resources 21 computing power 31 denial of arrive attacks, 41 ransomoware attack 51 Bizesin mining, etc	NA Low	r Low Low	r Local	Low	Low	None I	Inchanged	18 05	3.4	5.3	Low	62	38	Lysy 1. Identification of the sensitive data strange and excryption of storage subsystem 2. Standard Reveall 3. Relationing of the host system 3. Relationing of the host system of the standard	Security 2. SOM D001020115 - 13. Malwan Detection/Protection illy) 3. SAD/SDD-D001020099-6.7 Security 4. SOM D001020115 - 7.1. Access control policy and management	Document #: D001020037 Security Penetration Test Report: D001020164 DSTC001: GSL-STC-38	Low Low	Low Local	Low I	ow None	Unchanged	18	05 34	5.3	3.8 LOV	However, the individual risks were evaluated and reduced to ASAR to open the controls and	
Gaining Acress (ISTRED(E))	Unprotected metwork port(s) on network devices and connection points	Tablet OS/natwork details & Tablet Application A02	Ottain knowledge about system internuls Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnera Possibilities for exploitation of publicly known Vulnera		e None Low	r Network	Low	Low	None I	Inchanged	28 02	1.4	43	Low	02	2.0	Anti-virus with updated virus definitions Assit /System los conturins any	S. SAD/SIO-DO01020094-67 Security. wall 1.500 M001020115 - 13. Malwar Detection/Protection 2. SRS D001020024 - 2.17.6The physication shall support the use cantimulate mechanism id. SRS D001020024 - 2.21. The Application shall have logs of table application and firmware Conurthedic devices; 4. SRS D001020024 - 2.17.2The	Document #: D001020037 Security Penetration Test Report: D001020164 of DSTC001: GSL-STC-39	None None	Low Network	Low 1	ow None	Unchanged	28	0.2 1.4	4.3	2.0 LOV	Bith is broady acceptable since SomerMode: does not have residual risks in the Chical Bids (Parts) High Bids (Our Septon or in the Artical Bids (Parts) High Bids (Our Septon or in the Artical Bids (Parts) High Pinner Septon High Pinner Septo	120115 - 13. Malware Protection
29 Gaining Acress ((\$\frac{1}{2}\text{TREO}(\text{2}))	Unsprohected advances parely or and resources and connection points	Smart mode: App (Strybur Admir Web Application)	Clotain knowledge abver system internals Atmospt to find attack weekers Possibilities for exploitation of publicly known Vulnera Prossibilities for exploitation of publicly known Vulnera		e Low High	à Network	Low	Ngh	None I	Juchanged	12 67	42	55	Low	62	45	NAMES A Continue and the accessed higher conduction can be accessed higher conductation MATA. Mesons, serior preserved publicies & management and publicies & management and a continue and accessed accessed and accessed accessed and accessed acce	Application shall provide secure tunned Communications; channel by 1. Have to be closed before DR-8 2. SAN, SDD-0001020997 -2.17.4 The Application shall establish seclaric compromise to the integrity and confidentiality of health date of the confidentiality of health date of the other confidentials of the other c	Document #: D001020037 Security Preservation Test Report D001020164 at DTT0001-CSL-STC-40 di at seb	None Low	Low Network	Low 3	ligh None	Unchanged	12	04 25	38	2.8 LOV	Rida is broady acceptable done SmartMedic done on have residual rida is the Chical Bid. DELGA (Engl. Sign.) and the Chical Bid. Delca Sign. Sign	J20115 - 13. Malware Production
60 Gaining Access ([S]TRED(E]) TO3	Unproducted autwork port(s) on network devices and connection points	Tablet Resources - web cam, microphose, OTG devices, Removable USB, Tablet Removable USB, Tablet (Buetooth, Wife)	Chasin knowledge about system internuls Atmospt to find attack vectors Possibilities for exploitation of publicly known Vulnera Prossibilities for exploitation of publicly known Vulnera		e Low Nondo	e Network	Low	Low	Nome 1	Inchanged	28 02	. L4	43	Low	0.20	2.0	Anti-virus with updated virus definitions Audit/System log capturing any	wall 1. SOM D001020115 - 13. Malward Detection/Protection 2. SRS D001020024 - 2.17.6The Application shall support the use canti-malware mechanism	Document #: D001020037 Security Penetration Test Report: D001020164 of DSTC001: GSL-STC-41	None Low	None Network	Low 1	ow None	Unchanged	2.8	62 14	4.3	2.0 LOV	Bith it broady acceptable since Smarthedoc does not have residual data in the CRatal Table. Detection, the cond have residual data the CRatal Table. Detection, this (pethon) registers are in the declara this (pethon) register properties of the declara thin the control of the control of the control and reduced to APAT to ensure the controls and minjorine are adventory exalizated in the control of the back for an examina- tation of the control of the back for an examina- tation.	120115 - 13. Malware Protection
41 Gaining Accress (ESTRUMEES) T03	Devices with default passworth security in the control of the control of the security in the control of the control works from a structure of the works from a structure of the works from a structure of the control of the control of the works from a structure of the control of the control of the works from a structure of the control of the control of the works from a structure of the control of the control of the works from a structure of the control of the control of the works from a structure of the control of the control of the works from a structure of the control of the control of the works from a structure of the control of the control of the works from a structure of the control of the control of the works from a structure of the control of the control of the works from a structure of the control of the control of the control of the works from a structure of the control of the control of the control of the works from a structure of the control of	Authentication/Authorization method of all device(b)/app	Other is nowledge slowe system internals Other is nowledge, slowe system internals Other is nowledge, slower in the state of policy in the state of		r None High	a Physical	Low	Low	None 1	Jochanged	8.7 8.7	42	49	Moderate	0.50	4.6	Laburing the score providing of defaulted and the control of the c	tonnel Communications, channel I. Have to be closed before DR-8 by 2 SRS D001020023-2.1.2.2 If the Hospital Code is valid, then on pression the PROCEED button, the	Report D001020164 DSTC0001: GSL-STC-42 String alids	Low None	Low Physical	Low 1	ow None	Unchanged	67	0.4 2.5	32	29 LOV	Bits in harmonly compatible disser Seasontheader, done such have special size in the Cintail Bits (Each) Sligh Bits (code) regions or in the Medium Richi (priden): Proposition of the Medium Homeson, the Medium Homeson, the Medium Annual Proposition (APAT) to sensor the controls and vehicle the overall risks to the As Ear as Possible Levels.	
42 Gaining Access ([STFREE[12]) TIO	Devices with default passwords seeds to be checked for brusteforce attacks VOZ	Interface/APT Communication	Contain knowledge about system internals Atmospt to find attack vectors Possibilities for exploitation of publicly known Vulners Possibilities for exploitation of publicly known Vulners		r None Low	r Physical	Law	Low	None 1	Jachanged	0.7 0.4	25	12	Low	a2	נו	password is provided then immediate changing the password in needed. All the sense. I have been been been been been been been be	all: Have to be closed before DBLB 19. 2 SSED001020023-21-22 FM DBC001020023-21-22 FM Blcoplat Close is well, then on pressing the PECCEED harms, the validated by a switchine capital SSED001020077-21-25 The Applications shall be validated by a 1 A SSED001200077-21-21 TM SSED001200077-21-21 TM SSED001200077-21-21 TM SSED001200073-21-21 TM SSED001200073-21-21 TM SSED001200073-21-21 TM SSED001200077-21-21 TM 4 SSED001200077-21-21 Audit 4 SSED001200077-22-21 Audit 4 SSED001200077-22-21 Audit 5 SSED00120007-22-21 Audit 5 SSED00120007-22-	Document #: D001020037 Security Feneration Test Report D001020164 ab BSTC001: CSL-STC-44	Low None	Low Physical	Low I	ow None	Unchanged	0.7	84 25	32	2.7 LOV	Bids in broady acceptable sines SmartMedic does not have residual risks in the Critical Bids (Feld, Fillg Hold (coll regions or in the Redisam Bids (pricks) region. However, the indirectable risks were evaluated an important of the collection of the collection of the militageness are adequately exhibiting to the collection reduced to overall risks to the As far as Possible Levels.	
43 Garding Access (ESTREE(ES)) 703	The parameter completely or the pre-mile exhibits the wards parameter and hardcoded passwords.	Authoritication/Authoritation method of all forecept/japp	Chanda konolodga door oppen internals Others to the fall of the common of the		r None High	a Local	Low	Low	Required 1	Prochanged	13 67	42	5.6	Low	62	45	credentials & MFA. Thes, strong passwerd policies & management are required. 3. Limit authentication attempts (rain Limiting) 4. Auth/fysymm log. Melantial Access logs (logis (Limiting) 4. Mont/fysymm log. Melantial Access logs (logis (Limiting) & Malantial Access logs (logis action) & Malantial Access logis (logi	Hospital Lode is valid, then on pressing the PROCEED botton, the application shall be validated by the invisible captcha. (, id. SRS D001020097 - 2.1.2.6 The Application shall be validated by a function of the captch.	Presentation Testing Protects Decument #: D001020037 Security Presentation Testing Protects Report D0010201644 as DSTC001: GSL-STC-45 sing	Low Note	Low Local	Low 1	ow Required	Unchanged	13	0.4 2.5	39	28 LOV	Side in broady acceptable date Sauestheir, does not have reclosed this is the Cartical Bidd (Bad) Sligh Bidd (Ged) regions or the Medium Ridd (Bad) Sligh Bidd (Ged) regions or the Medium Ridd (Ridd) Sligh Bidd (Red) Sligh Bidd (Red) Sligh Bidd (Red) Slight Bidd (R	
44 Gaining Access (GSPHERIGE)) VB3	Decking anthentication modes for possible hards and Typessen.	Authentication/Authentication method of all forecept/pape	Obtain konsledge door opgen internals Obtain konsledge door opgen internals Obtains to third gath on yours Presidents for exploitation of publicly known Yulners Presidents for exploitation of publicly known Yulners	NA NA Lova	r Low Low	r Physical	Low	Low	None I	Technaged	87 65	34	ei ei	Low	02	26	protocol attacks 2. Encrypt authentication data using neversible encryption such as using a digost (e.g., RASSI) and a seed to preve dictionary attacks 3. Lock out accounts after reaching a londing the distinct of the di	fision me feature for logic credentials a all the data which we shall see one inside local storage shall be encrypted. SAD/SDD-D001020099-6.7 Securion SRS D0010200272-213:25ystem shall tackion.	Security Prestration Test Report D00101646 DSTC001-GSL-STC-48 proper D00101647 proper D00101647	Low Low	Low Physical	Low I	ew None	Unchanged	87	05 34	а	3.6 LOV	Risk in hready acceptable dines famesthetic does not have excluded at the 16th Critical Risk (Rad Shigh Risk (Gen Feigine or in the Medium Risk (pollow) region. However, the individual risks were evaluated and reduced to MAPA to ensure the controls and mitigations are adopted by the control of the adopted at the control of the control of the adopted at the control of the control of the adopted at the control of the control of the control of the control of the control of the control of the control of the control of the contro	

Revision: AB Form																												
			Adverse Impact	nity	6					Pre-in	mplementation of Security Contro	s						Security Controls/Mitigations		lity.	,			Post-Implementati	on of Security Controls			
ID # Threat Event(s)	Vulnerabilities	Asset	Impact Description	Safety Impact (Risk ID# or N/A)	Integrity Availabilis	Attack Vector	Attack Complexity	Privileges Required	iser Interaction	Scope Exp	ploitability Sub Score ISC Base	Impact Sub Score	CVSS v3.0 Base Score	Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score		Measures	d Verification of Risk Control Measures (Effectiveness)	Confidentia	Attack Vector	Attack Privi Complexity Requ	leges User ired Interaction	Scope Exploitable Score	ility Sub ISC Base I	Score CVSS v3.0 Base Score	Overall Risk Sec	urity Risk Residual Security Risk Acceptability Remarks (Column added additionally to SOM Reference
65 Gaining Access (STMING(I)) THE	Charking unthemeration modes for possible hacks and bypanuss	Statet medic app (Stryker Admin Web Application)	Otherin knowledge above system internals: Atmaps for all early-vectors Possibilities for exploitation of publicly known Vulnera.		r Low Low	Physical	Low	Low	None U	fochanged	0.7	34	ti.	Low	0.2	36	2. Encrypt authentication data using non reversible encryption such as using a digest (e.g., RASH) and a seed to prevent dictionary attacks. 3. Lock out accounts after reaching a log on failure threshold and mitigate risk of brate force attacks. 4. Display generic error messages upon validation of credentiats to mitigate risk.	on me feature for login credentials and all the data which we shall store inside local storage shall be encrypted. SAD/SDD-D001020099-6.7 Security 5 SAD/SDD-D001020099-6.7 Security 6	d Security Penetration Test Report: D001020164 DSTC001: GSL-STC-49	Low Low 1	.ow Physical	Low L	w None	Unchanged 0.3	e as	34 41	36	Rich to brookly acceptable does not have deaded offered to the contract of the
66 Gaining Access (STREEGE) T03	Oxeding sufferitiestion modes for promites backs and typusons for possible backs and typusons VOI	Smart medic app (Amere Portal Administratory)	Obtain knowledge about system internals Atmaptes that datase vectors Presidents for explications of publicly known Volume		r Low Low	Physical	Low	Low	None U	Inchanged	87 85	2.4	41	Low	62	16	E.OW 1. Encrypt the authentication data is necessary to be authentication data in the result of the continue o	Something went swrong with API operation try again / contact API admin. The setup-& configuration process came cloud & admin shall be continued to the continued of the continu	Document #: D001020037 he Security Penetration Test	Low Low 1	.ow Physical	Low L	rw None	Unchanged 0.2	es es	34 41	3.6	Bish is broughy acceptable since Smorthedic decembers on these resident design in the Original Bish decembers of the Original Bish decembers (bish of the Original Bish decembers (bish of the Original Bish decembers). However, the individual disk were evaluated and reduced the AIP to ensure the contributed and reduced the AIP to ensure the contributed and insignation are adequately appealable to the contributed of the Original Bish decembers of the Original Bis
Gaining Access (ISTRUD(IS))	Unproducted external USB Part on the tablet/devices.	Tablet Resources - web cam, nicrophene, OTC devices, Removable USR, Tablet Application, Network interfaces (Illustrooth, Wiff)	Otdain havedredge about system internals Atmospt to find attack vectors Possibilities for exploitation of publicly known Vulnera Possibilities for exploitation of publicly known Vulnera		r Low Low	Physical	Low	Low	Required U	inchanged	es es	34	39	Low	62	15	LOW 1. Asser should be behind stateful firewar 2. Anti-virus with updated virus defailations 3. Antif. (System log capturing any shoromal activity identified /reported by the application 6. 1 be hordered interfaces (n/w) 8.	all 1.50M D001020115 - 13. Mahusre Detection/Protection 2. SISS D001020024 - 2.17.6The / Applications built support the use of anti-mahusre mechanism 3. SISS D0010200024 - 2.21. The Application that have tops of tablet applications and firmulare (SmartMedic devices) 4. SISS D0010200024 - 2.17. The Application shall provide soccure	Document #: D001020037 Security Penetration Test Report: D001020164 DSTC001: GSL-STC-53	Low Low 1	.ow Physical	Low L	w Required	Unchanged 0.5	. 0.5	3.4 39	25	Bids is broudy acceptable since Smarthediz floor, so of the versible of disks in the Critical Bids (Pacts, Sign Pacts) (seed persistent of the Sign Bids (Pacts, Sign Pacts) (seed persistent on the Martin Bids (Pacts) (seed persistent of the Martin Bids (Pacts) (seed persistent Bids) Blowever, the individuals risks were evaluated and reduced to AFAP we seemen the ceitrish and Levis. Levis. Levis.
40 Materialising Access (TTY)	Devices with default passwoods as eased to be decided for brokelstere attacks for translations attacks for Vdz.	Authoristic action / further-reastons method of all device(ty)/app	10 Ottain knowledge about system internals: 20 Attempt for find after wetters 32 Attempt for find after wetters 37 Passibilities for exploitation of publicly known Vulnera.		: Low Low	Physical	Low	Low	None U	fochunged	87 85	24	41	Moderate	85	24	1509 1. During the across providing if default parameter is provided from immediately thought the parameter of a needed. 2. Require multi-decire administration in 1. Linit archemistrations already in 1. Linit archemistration archemistration in 1. Linit archemistration archemistration archemistration archemistration archemistration methods 5. Stronger authentication methods	Hospital Code is valid, then on pressing the PROCEED button, the application shall be validated by the invisible captcha SRS D001020097 - 2.1.2.6 The d Application shall be validated by usi invisible captcha during login. 3 SRS D001020097 - 2.1.3 I Invalidated SRS D001020097 - 2.1.3 I Invalidated SRS D001020097 - 2.1.3 Invalidated SRS D001020	Security Penetration Test Report D00120164 DSTC001: GSL-STC-S6	Low Low 1	.cow Physical	Low L	w None	Unchanged 6.3	0.5	34 41	38	this is brough acceptable time on Smart Medic does not flow vesible of this in the Cities Black (Party Sligh Bird (vel) rejection or in the Medician Life, rejection). The cities are selected as the contract of the contract of the cities of the cities of the cities of the Borevere, the inflictional risks were evaluated as the cities of the cities of the cities of the cities of the instigations are adoptically vestable to the reduce the overall risks to the As far as Fundble Levels.
69 Maintaining Acress (TTP) 1704	The password complexity or functions withouthing; this work password and hardcoaled passwords.	Authoritication / Authorisation method of all device (§) / app	Dithein browledge above system internals Atmospt to find attack vectors Possibilities for exploitations of publicly known Vulnera Prossibilities for exploitations of publicly known Vulnera		r Low Low	Local	Low	Low	Required U	fochanged	13 85	14	48	Low	62	17	password policies & north, strong password policies & management are required 2. Require multi-factor authentication 3. Limit authentication attempts (rate Limiting) 4. Audif, Plystem log - Maintain Access logs (logic Litempted & failed), logoff, idchange)	d SRS D001020097 - 2.1.2.6 The Application shall be validated by usi	Security Prescriptions Fluid Report D001020144 DSTC001. CSL-STC-S9	Low Low 1	.ow Local	Low L	ow Required	Unchanged 1.3	as as	34 48	1,7	Rick is brough acceptable since SeautMedie Gene on the re-residued ricks in the Critical Rick (Roch Silling Rick) (rick) regions or in the Medium Rick (primits) regions. However, the Individual ricks were evaluated an interpretation of the Rick (Roch Rick) (Roch Rick) and Rick (Roch Rick) (Roch Rick) and Rick (Roch Rick) a
50 Charring Truck (TTP) T05	Indicare Configuration for Software (Of the Model Devices, Lajutops, Workstations, and Servers V22	Tablet Resources - web case, microphone, OTC devices, Removable USR Tablet Application, Newton's interfaces (Illustrooth, Wiff)	1) Tumpering of forestic data 2) This involves modifying (corrupting) (deleting the values 3) Modifying registry values (1) Modifying registry values (5) Deleting at fielders which were created		r Low Low	Local	Low	Low	Required U	inchanged	13 05	34	45	Low	62	37	definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) &	6. SAD/SDD-D001020099-6.7 Solution Solution (Protection 2. SIS D0010200115-13. Malware betection (Protection 2. SIS D001020024-2-17.6The paginization shall support the use of anti-malware mechanism 3.SIS D001020024-2-22.1 The Application shall have logs of tablet application and firmware Sisant/Madic devices) 4. SIS D001020024-2-17.2The		Low Low 1	.ow Local	Low L	ow Required	Unchanged 1.3	: as	3.4 4.8	13	Eich is braudy acceptable since Sourchedel: does not have residual risks in the Critical Risk (Part) Risk Risk (red) region or in the Medium Risk (Risk Risk (red)) region or in the Medium Risk (red) region or in the Medium Ris
S1 Cheming Track (TTP)	Outdated - Software/Hardware V23	101	2) This involves modifying/corrupting/defining the values 2) Modifying registry values split.action (Train 3) Modifying registry values split.action (Train 3) Deleting all fidders which were created	D001020010) Low	r Low Love	Physical	Low	Low	None U	inchanged	6.7 6.5	34	41	Moderate	e .5	38	 Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by 	Detection/Protection 2 SRS D001020024-2-17.6The y Application shall support the use of anti-malware mechanism 3 SRS D001020024-2-23.1 The Application shall have logs of tablet application and firmware SimutiMedic devices]. 4 SRS D001020024-2-17.2The Application shall provide secure remost Communications channels	DSTC001: GSL-STC-66	Low Low 1	.ow Physical	Low La	ver None	Unchanged 0.2	. 05	3.4 4.1	38	Eisk is broudy acceptable since Sinut/Medic does not have residual risks in the Critical Bild Description of the Critical Bild Levis. Low Description are adoquirably restablished to reduce the event of risks to the As far as Possible Levis.
S2 Coarsing Track (TTP) T05	Lake for Configuration controls for T assets in the information system plan	(Bluetooth, Wiff)	1) Timepring of forestic data 2) This involves modifying corrupting/defecting the values 3) Modifying opigitary values 4) Modifying opigitary values 4) Winterstanding and involves splitted involves opigitariously object of the control of the control opigitariously object of the control opigitariously objec	SmartMedic Document # D001020010)	r Low Low	Local	Low	Low	Required U	Inchanged	13 65	34	48	Low	0.2	17	Use hardened interfaces (n/w) & secure tunnel communications channel	II 1. SOM D001020115 - 13. Malware Detection/Protection	Bocument 8: D001/00037 Security Princitation Test Report: D001020164 DSTC001: GSL-STC-67	Low Low 1	iow Local	Low L	ow Required	Unchanged 1.3	: 0.5	3.4 4.8	33	Sick is knowly acceptable does foundeduction. Also with the Workship of the State
S3 Georing Track (TTP) TOS	Lack of configuration controls for IT assets in the information system plan	Device Maintainence tool (Hardware/Software)	1) Tampering of forensis data 2) This involves modifying/corrupting/defeting the values 3) Modifying registry values 4) Unincealling all macious applications/hools 5) Deleting all folders which were created	Risk Table and Risk Matrix	r Low Low	Local	Low	Low	Required U	Inchanged	13 05	34	48	Low	0.2	3.7	LOW 1. Assort should be behind stateful firewal 2. Activities with updated virus definitions 3. Audiffysystem log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	all Device maintainence tool not implemented/existing in the SM platform.	Penetration Testing Protocol Document #: D001020037 Security Penetration Test Report: D001020164 DSTC001: GSL-STC-68	Low Low 1	low Local	Low L	w Required	Unchanged 1.3	0.5	3.4 4.8	37	Bids it breastly acceptables since SmartMedic does not have residual risks in the Citabil Bids (Bids). Bigh Bids (near) regions or in the Mendman Bids (throit) regions. LOW However, the individual risks were evaluanted and reflexed to AFAF to ensure who the controls and minigations are adequately restablished to violus the evalual risks to the AFAF to stress the art Permission violus the evalual risks to the AFAF to ensure as a Permission
54 Obering Track (TTP) TOS	Ineffective patch management of fireway. Os and applications thoughout the information system plan	101	3) Tampering of forensic data 2) This involves modifying/corrupting/fide/tring the values 3) Modifying registry values 4) Modifying registry values 5) Deleting all folders which were created 5) Deleting all folders which were created	DOUINSHE # DO01020010) Nons	e Low Low	Local	Low	High	None U	Inchanged	0.8 0.4	25	3.6	Moderate	0.5	30	Low 2. A lower should be should standed frewal 2. Asked view with updated with a definitions at 3. Audit System lag capturing any absonemal activity identifications produced activity identification projects of the application interfaces (system) 4. One handward interfaces (system) 4. One handward interfaces (system) 4. We will be applicated to interfaces (system) 4. We will be applicated interface (system) 4. We will be applicated interfaces (system) 4. We will be applicated interface (system) 4. We will be applicated interfaces (system) 4. We will be app	2. SRS D001020024 - 2.17.6The Application shall support the use of anti-mahware mechanism		None Low 1	.ow Local	Low H	gh None	Unchanged 0.8	: 0.4	2.5 3.4	30	This is broady acceptable into Faster State Periods: does not have whealed risks in the Clark Book Book Book Book Book Book Book Bo
SS Clearing Track (TTP) TOS	Ineffective patch management of feware, CS and applications thoughout the information system plan	Device Maintainence tool (Hardware/Software)	Tampering of forensic data This involves modifying corrupting/deleting the values Modifying registry values Homerstalling all malicious applications/tools Deleting all folders which were created		r Low Low	Local	Low	Low	None U	Inchanged	1.8 0.5	3.4	53	Low	0.2	3.8	LOW Loses should be behind stateful firewal 2. Assis-was with updated virus definitions 3. Audit/System log capturing any absormal activity identified/reported by the application 4. Use hardenest interfaces (n/w) & secure tunnel communications channel	 Device maintainence tool not implemented/existing in the SM platform. 	Penetration Testing Protocol Document 8: D001020037 Security Penetration Test Report: D001020164 DSTC001: GSL-STC-70	Low Low 1	iew Local	Low L	w None	Unchanged 1.8	0.5	3.4 53	3.8	Bill is bready acceptable since StaurMedic does not have residual risks in the Citatical Bill (Bild,) Billy Bild (red) region or at the Medium Bild, Yellor) region. LOW Blowwort, the individual risks were evaluated and reflected to AFAP to ensure the controlle and minigations are adequately established to relate the residual risks since the set as Possible related to the Processing of the Processing of the Pro-
56 Gearling Track (TTP) TUS	Inaffective patch mesagement of flowers. Of and applications thoughout the information system plan	Tählet OS/introork details & Tählet Application	1) Tumpering of foreints data 2) This involves modifying (corrupta)/deleting the values 2) This involves modifying (corrupta)/deleting the values 3) Modifying quigitary in Modifying control to the state of the sta	Risk Matrix SmartMedic Document # D0010200101	r Low Low	Local	Love	Low	None U	Inchanged	1.8 0.5	24	53	Low	0.2	18	abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & come based on a superiorities choused	SRS D001020024-2-17.6The Application shall support the use of anti-matheure mechanism SSRS D001020024-2-22.1 The Application shall have logs of tablet application and firmware (Smarthéedic devices). 4. SRS D001020024-2-17.2The	Security Penetration Test Report: D001020164 DSTC001: GSL-STC-71	Low Low 1	Local	Low L	w None	Unchanged 1.8	0.5	3.4 53	38	Levols. Eink is brooky acceptable since Smurtheder Since Index or there resided risks in the Critical Side Side since there resided risks in the Critical Side Side (Smort) region sizes on the brook Side Side Side Side Side Side Side Side
57 Clearing Track (TTP) TWS	The static connection digarram between devices and applications of applications of the state of	Device Maintainence tool (Bartheare/Software)	Transporting of forensic data This involves modifying/corrupting/deleting the values This involves modifying/corrupting/deleting the values Modifying registry-values applications/transls Deleting all fielders which were created	Risk Matrix SmartMedic	r Low Low	Local	Low	Low	None U	Inchanged	18 65	34	53	Low	0.2	38	Lower dwald be behind stastful flowers Assist with updated virus Assist with updated virus Assist process on the control of the control Assist process no quagrating any abnormal activity identified/properate by the application Use hardened interfaces (n/w) & secure tunned communications channel	plotform	Penetration Testing Protocol Document 8: D001020037 Security Penetration Test Report D001020164 DSTC001: GSL-STC-72	Low Low 1	Local	Low L	w None	Unchanged 1.8	0.5	3.4 5.3	38	Bild is brassly acceptable since Stear Ordele: Geos not have residual risks in the Critical Bild (Rods) Right (level) regions or in the Medium fails (pridies) regions; (level) regions or in the Medium fails (pridies) regions. However, the Individual risks were evaluated and reduced in ARM's sensors the cointin hand when the reversal risks to the Art far as Possible Levels.

Form			Adverse Impact		b						P	Pre-Implementation of Secu	ity Controls						Security Controls/Mitigations		2					Post-Implementatio	n of Security Controls			
ID # Threat Event(s)	Vulnerabilities	Asset	Impact Description	Safety Impact (Risk ID# or N/A)	Confidentiali	Integrity Availability	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Exploitability Sub Score	ISC Base Impact Sub S	ore CVSS v3.0 Base Scot	re Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score	Level	Measures	ol Verification of Risk Control Measures (Effectiveness)	Confidentiali Integrity	Attack Vector	Attack Complexity	Privileges Required	User Interaction S	cope Exploitabil	ity Sub ISC Base	Impact Sub Score Base Sc	3.0 Overall Risk ore Score	Security Risk Residual Security Risk Acceptability Remarks (Column added a SOM Reference
S8 Clearing Track (TTP)	The static connection diguram between devices and applications with provision for periodic updation as per changes V10 A		1) Tampering of forensic data 1) Tampering of Tambering of Services of the Se	B- L2(Reference Rick Table and Rick Marrix SmartMedic Document # D001020010)		Low Low	Local	Low	Low	None	Unchanged	1.8	0.5 3.4	53	Low	0.2	38	2. Anti-virus with updated virus definitions 3. Andit/System log capturing any abnormal activity identified/reported the application 4. Use hardened interfaces (n/w) &	wall ISOM D00102015-13 Mahwa Debettion (Protection U.S. SES D001020024-217.6The Papilication shall support the use- anti-mahware mechanism el 3.885 D001020024-223.1 The Applications shall have logs of table applications shall have logs of table applications of the control of the control of the control (Immt Medic device).	Document #: D001020037 Security Penetration Test Report: D001020164 f DSTC001: GSL-STC-73	Low Low	Low Local	Low	Low	None Un	changed 1.8	0.5	3.4 5.3	38	Bild is bready acceptable sines Smarthede does not have residual risks in the Criscil Risk (Red.) Risk Risk (red.) regions or in the Medium Risk (price) region. However, the individual risks were evaluated and reflaced to ARAP to ensure the controls and militagitions are adequately restablished to reduce the overall risks to the Ast for an Provible Levels.
59 Elevation of privilege (STRUD(E]) T06	Controlled Use of Administrative Privileges over the network V2S	method of all device(s)/app	I) Galaning access to the portal I) Accessing confidential data, I) Load misses of confidential data (Company defanation	NA NA	Low	Low Low	Network	Low	Low	Required	Unchanged	2.1	0.5 3.4	5.5	Low	02	38	administrator and non-administrative accounts. 2. Access to a machine (either remotel or locally) should be blocked for administrator level accounts.	Application shall provide secure tunned Communications channel sh 1885 D001020023-21.22 if the Hospital Code is valid, then on pressing the PROCEED button, the application shall be validated by it invisible captcha SRS D001020097 - 2.1.2.6 The Application shall be validated by invisible captcha during logarity	BETCOOL: GSL-STC-74	Low Low	Low Network	Low	Low	Required Un	changed 2.1	0.5	3.4 5.1	3.8	Suit is branchy acceptable dates four-the-fe- done on how revised and talks in the Critical Stak (Bod.) High Rinks (perly spins on the Medium Rink (perlison) regions. However, the individual risks were evaluated and reduced to MAT's to ensure the controls and missing are acceptable to the spin of the controls and missing are acceptable to the Art or it is to be a few and to Low.
60 Elevation of privilege (STRID(E)) T06	Controlled Use of Administrative Privileges over the network VSS A	Smart medic app (Azure Portal Administrator) 12] Caining access to the portal] Accessing confidential data,] Accessing Confidential data] Lead mission of Confidential data () Company defamation	NA.	None	Low High	Network	Low	High	Required	Unchanged	0.9	07 42	52	Moderate	0.5	4.7	MEDIUM 1. Require that administrators establish multi factor authentication for this individual factor authentication for the individual reasons. 2. Access to a machine (either remote accesses. 2. Access to a machine (either remote administrator) are developed accesses. 3. Ensure defaults created nature and authentication of the accesses for any autot (tout in applications, operating systems, restort, factor).	3. Have to be closed before DR-8 sh The setup & configuration processarure cloud & admin shall be documented and published within organization for the correspondit teams using the admin portal	of Penetration Testing Protocol	None Low	Low Network	Low	High	Required Un	changed 0.9	0.4	2.5 3.1	3.0	this is broadly recordable design from 1984a; done one have revoluted ricks in the C friend Black (Rod.) High Black (red.) regions or in the Medium Black (reflect) regions. However, the individual ricks were evaluated and reflected to MAPE to remove the extends and mingetima are adequately established to any or the extends and the second recordable and mingetima are adequately established to be a record ricks to the first or a Provided Levels.
61 Denial of service (STRAID JE) TO7	Unprotected network part(s) on instructed divices and connection points V22	Tablet OS/natwork details & Tablet Application	() Bring down the service availability [Bitcking the end user usage	NA.	None	None High	Network	Low	Low	None	Unchanged	2.8	0.6 1.6	6.5	Low	0.2	42	wereless access points). MEDIUM 1. Asset should be behind started free? 2. Asst-virus with updated virus definitions 3. System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces in /w / &	usul 1. SOM D001020115 - 13. Mahwas Debection / Protection Debection / Protection 1 2. SRS D001020024 - 2.7.6 The Application shall support the use-anti-mahware mechanism shall support the use-anti-mahware mechanism shall support the use-anti-mahware and shall have logic of and application shall have logic of and application shall have logic of and application shall have logic of and (EmartMedic devices).	Document #: D001020037 Security Penetration Text Report: D001020164 f DSTC001: GSL-STC-77	None None	Low Network	Low	Low	None Un	changed 2.8	0.2	1.4 4.3	2.0	Bild is bready acceptable since StaurMedic does not have vesidant risks in the Critical Bild. (Bod) light Bild (evel) region in the Medium Bild (printer) region. However, first individual risks were evaluated and reduced to ARA to ensure the contributed for the overall risks to the Art on Provided reduced to the overall risks to the Art on Provided Levels.
62 Information disclosure (STR(1906)	Unexactlypted data at east in all possible locations at east in all possible locations	Data at Rest I	information of habitilities can be explore and ducks make the explore and ducks makes like not records, tables six.	ose with various NA	Low	Low Low	Local	High	High	None	Unchanged	0.5	05 34	39	Moderate	85	37	Low 1. Mentification of the certainty data disrept and exception of through subjection of through subjection and the certain of the certain and the certain an	4. SSE D001020077 - 21.2 TJM Application shift provide secure 10. 1. SSE D001020077 - 21.1 ZJM Application shift was the Tarmen and Funtation for legisla creditarities, and applications shift was the Tarmen and Funtation for legisla creditarities, and saidle local transport shift be energypted. 2. SSE D001020077 - 2. SSE Z-SSE D001020077 - 2. ZSI Application shift have the User Management Extrem to configure the Management Extrem to the textrem to configure the Management Extrem to configure the Management Extrem to configure the Management Extrem to configure the Mana	ber Document #: D001020037 Security Frentration Test Report D001020164 DSTC001: GSL-STC-78)	Low Low	Lew Lecal	High	High	None Un	changed 0.5	0.5	24 25	37	Rails to branchy accordable desire Researche. does not have resident drike in the Critical Rails. (Red.) Eligh. Rails (pell-or) gene in the Medium. Rills (primor) region. However, the individual rills were evaluated militagitimes are adequately exalizable to a reduce the overall risks to the Act for an Possible Level. LOW
63 Information disclosure (STR(1902)	Unanceypted data in transit in all flowchamnels	Data in Transit I	usformation of health, data can be exploit and disclo- neases like network; tables sit.	ose with various NA	Low	None Low	Network	High	Low	None	Unchanged	1.6	84 25	42	Moderate	85	3.4	1. Use sectors hannel communications channel 2. Configure and upge pade renders for a few security as we security as we security as the security practice with product all devices. 4. Maintain access control (rend/mod permissions land for any persistent land for any security sec	1. SIS D001020024-2.17.2The Application shall provide neces than 4 Communication channel SIS D001020023-2.13.2The Application shall provide neces ulty) 2. SOM D001020115-72. 2. Trainmission confidentially in 3. SOM D001020115-13. Malwar D00100107. Access 4. SOM D001020115-1. Access 4. SOM D001020115-1. Access	Penetration Testing Protocol Document #: D001020037 Security Penetration Test Report D001020164 DSTC001: GSL-STC-79	Low None	Low Network	High	Low	None Un	changed 1.6	0.4	2.5 4.2	3.4	Bile is broady acceptable sizes SmartMedic does not have visibal and talks in the Chical Risk (Rod.) High Risk (red) region or in the Medium Risk (price) region or in the Medium Risk (price) region. However, the individual risks were evaluated and reduced to ARPA to ensure the controls and 5.50M D001020115-7.1. militage are adequately exhibited to militage are an edequately exhibited to militage the everal risks to the Art for a Penulte factor.
64 Information disclosure (CTR(s)00)	Weak Encryption Implementation in data acres and in some trackets and designs were started and designs were started and designs were started and designs were started as a second and designs were started as a second and designs were started as a second as a s	Outra at Rest I	information of health data can be exploit and disclosures the ractives it, tables exc	now with various NA	Low	Low Low	Local	High	High	None	Unchanged	ū.s	Q5 34	35	Moderate	as	37	using Service-Managed keys/recomer practise by azure. 2. Proper way of network access conti	2 SOM D001020115 - 7.1. Access nsit, control policy and management 3. SAD/SDD-D001020099-6.7 Security	Document 8: D00120037 Security Pieratrization Test Report D001020164 DSTC001: CSL-SYC-80 Urity y	Low Low	Low Local	High	High	None Un	changed 0.5	0.5	24 25	37	Blak is broady acceptable dince SmarMode: (Rod) lingh link (red) regions or in the Medium Blak (price) region. However, the infinitedant risks were evaluated and reduced to MAPP to remote the custods and mitigations are adequately seathfolds to ever the control of the control and mitigations are shown to the Art or remote Levels.
65 Information duclosure (STR(()0X) T08	Weak Encryption Implementation in data at ever and in transit sactical and design wise	Date in Transit (referencies or bruth data can be exploit and disclosure because the retwork, tables etc	ose with various NA	Low	None Low	Network	High	Low	None	Unchanged	1.6	04 25	Q	Moderate	85	34	Low L. Standard Enewall 2. Configure and opprade routers for a Configure and opprade routers for a Configure Teresists to reject any packets with spended address. 4. The secure based communication channel.	2. SOM D001020115 - 22. Transmission confidentiality	Document #: D001020037 Security Penetration Test Report: D001020164 DSTC001: GSL-STC-81	Low None	Low Network	High	Low	None Un	thanged 1.6	0.4	25 4.	3.4	Bluk is broadly acceptable since SmartMedic does on have vanished rinks a the Critical Bluk Blue Committee vanished rinks as the Critical Bluk Blue Committee Committe
66 Information disclosure (STR(I)DE)	Weak Algorithm implementation with respect cipher key size V29		reformation of health data can be exploit and disclo- neans like network, tablet etc	ose with various NA	Low	Low Low	Local	High	High	None	Unchanged	0.5	0.5 3.4	39	Moderate	0.5	3.7		tc between browser application and backend. 6 Sic. 2 SRS D001020097 –2.8.1Application and shall use APIs to communicate between browser application and	Document #: D001020037 the Security Penetration Test Report: D001020164 tion DSTC001: GSL-STC-82	Low Low	Low Local	High	High	None Un	changed 0.5	0.5	3.4 3.9	3.7	Each is broasely acceptable store SmartMode. (Rod.) Righ Risk (red.) regions or in the Medium Bild (rollow) regions or in the Medium Bild (rollow) region. LOW LOW LOW LOW LOW LOW LOW LO
67 Information disclosure (STR(I)DE) TOS Information disclosure	Weak Algorithm implementation with respect cipher key sine V19 A	10	nformation of health data can be exploit and discineans like network, tablet etc If the network is the second of the network is the network of the network is the network of the network is not discine to the network is not the network in the network in the network is not the network in		Low	None Low	Network	High	Low	None	Unchanged	1.6	0.4 2.5	42	Moderate	0.5	3.4	etc. should be avoided and urage of strong algorithms such as AES, RSA, et are recomended 2. Typical key lengths are 128 and 25- bits for private keys and 2048 for pub- keys are recommended.		Document #: D001020037 Security Penetration Test Report D001020164 tion DSTC001: GSL-STC-83 the	Low None	Low Network	High	Low	None Uni	changed 1.6	0.4	25 42	3.4	Levek. Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red.) High Risk (red) region or in the Medium Risk (yellow) region.
(STRE(JDE)	Inforcers Configuration for Software Configuration for Software (Software Con Mobile Devices, Laptops, Workstations, and Stervers V22	Table Beseucces - web cam, microphone, Ord-devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	offormation of health data can be exploit and discho neans like serwork; tablet etc.		Low	Low Low	Network	High	High	None	Unchanged	0.7	0.5 3.4	41	Moderate	es	3.8	defusitions 3. Audit/System log capturing any abnormal activity identified/reported the application identified/reported by application 4. Use hardened interfaces (n/w) &	2-SRS D001020024-2-17.6 The application shall support the use-than and substrained materials with a special shall support the use-than and substrained materials with a special shall have logs of table application and firmware (SmartMedic devices). 4-SRS D001020024-2-17.2 The Applications shall provide secure Applications thall provide secure.	Report: D001020164 f DSTC001: GSL-STC-84	Low Low	Low Network	High	High	None Un	changed 0.7	0.5	3.4 4.1	38	does not have vesichal richis in the Criscial Biol. (Bod.) High Biol. (evel you good in the Medium Biol. (crimino) region. Hill Confined y region. Hill were fire in distributal richis were evaluated and richieved to AFA to remore the control and LOW went on the overall richis to the As far as Possible Lovel.
69 Information disclosure (STR(1)0C) T06	Unencrypted Network segment through our the information flow	Data in Transit 1	asformation of health data can be exploit and disclusions. But serbooth, tablerest:	ose with various NA	Low	None Low	Network	High	Low	None	Unchanged	1.6	0.4 2.5	42	Moderate	ēS .	3.4	Change) A Audit /System Inc., Maintain securit	tunnel Communications channel 1.SRS D001020023-2.1.6.21The application shall allow to assign a edit patient reference ID to patie	Report D001020164 DSTC001: GSL-STC-85 by	Low None	Low Network	High	Low	None Un	thanged 1.6	0.4	25 4	3.4	talk it heready accordable desics flowerModel; doine on the we reduced and talk in the Critical Bids (Bods) life, Bids (red v) light Bids were evaluated, and reduced to ARAT to ensure the controls and militagitions are adequately settledded to reduce the overall risks to the Aid far as Promittle Levil. LOW
																			4.SRS D001020024-2-23.1 The Application shall have logs of tabl application and firmware (SmartMedic devices).	ıt.										

			Adverse Impact							Pi	're-Implementation of Secur	ty Controls						Security Controls/Mitigations						Post-	Implementation of Sec	urity Controls			
Threat Event(s)	Vulnerabilities	Asset	Impact Description	Safety Impact (Risk ID# or N/A)	Integrity vailability	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope	Exploitability Sub Score	ISC Base Impact Sub Sc	re CVSS v3.0 Base Score	Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score	curity lisk Security Risk Control Measures evel	Implementation of Risk Control Measures	Verification of Risk Control Measures (Effectiveness)	mfide ntiality Integrify vailability	Attack Vector	Attack Pr Complexity Re	vileges Use uired Interact	r ion Scope	Exploitability Sub Score	ISC Base Impa	ct Sub CVSS v3.0 re Base Score	Overall Risk Score	Security Risk Residual Security Risk Acceptability Remarks (Column added SOM Reference
Information disclosure (STR(I)DE)	Insecure communications in networks (hospital)	Data in Transit	Information of health data can be exploit and disclose with various means like activorit, tablet etc	NA S													OW 1. Secure communication with Secure Sockets Layer (SS.) or TLS protocols provide message confidentially 2. Secure sensitive data in the channel flow using strong encryption 3. Stateful firewall 4. Proper way of network access confidential for the confidential firewall 5.	2. SAD/SDD-D001020099-6.7 Security	Penetration Testing Protocol Document #: D001020037 Security Fenetration Test Report: D001020164 DSTC001: GSL-STC-86	3 <									Bind is broadly acceptable since SmartShede: there not have revealed affects the Critical Fish. Detection/Protection Bild (yellow) region. Bild (yellow) r
8	VOS	A10		Lov	r None Low	Network	High	Low	None	Unchanged	1.6	8.4 2.5	42	Moderate	e 5	3.4		4. SOM D001020115 - 7.1. Access control policy and management		Low None Low	v Network	High	Low Non	e Unchanged	1.6	0.4	5 42	3.4	LOW
Data Access (STR(I)DE)	Unprotected network port(s) on serverok devices and connection points	Tablet Besources - web cam, microphose, OTG devices, Application, Network interfaces (Biostooth, Wiff)	Allowing application or script to perform abnormal activities on the 1 option. J. Modifying the data, tamporing the confidential data making it is associated or challenging the integrity of data.		e None High	Network	High	High	None	Unchanged	0.7	0.6 1.6	44	Low	0.2	38	Anti-virus with updated virus definitions Audit/System log capturing any	and 1.50M 0001020115-13. Malware Detection/Protection Detection/Protection by Spilland Spilla	Document #: D001020037 Security Penetration Test Report: D001020164 DSTC001: GSL-STC-87	None None Low	r Network	High	High Non	e Unchanged	0.7	0.2	.4 22	1.6	Solis is broady acceptable since StauesMedic does not have residual fields in the Critical Bids (Bods) High Bids (eds) prigate or How Medium Rich (pull-my) region. However, the individual rich six were evaluated and reduced to MAP to ensure the controls and control to the co
Data Access (STR[I]DE)	Unprotected network port(s) on astroorf: devices and connection points	Tablet OS/network details & Tablet Application Application	Allowing application or script to perform abnormal activities on the 1 years years years man and the script of		e Low Low	Network	High	High	None	Unchanged	8.7	84 25	33	Low	02	27	the application 4. Use hardened interfaces (n/w) &	usal 1.50M D001020115-13. Malware Datection/Protection 2.SRS D001020024-2-17.6 The by Application shall support the use of anti-malware merchanism 3.SRS D001020024-2-22.1 The Application shall have logs of tablet application and firmmare (Emarthédic devices). 4.SRS D001000024-2.17.2 The Application shall provide society tunned (Communications channel accure tunned (Communications channel).	Document #: D001020037 Security Penetration Test Report: D001020164 DSTC001: GSL-STC-89	None Low Low	r Network	High	High Non	e Unchanged	0.7	0.4	5 33	2.7	Bids is broadly acceptable since Smart Medic dies on their residuals find Collect Rick Most Collection Rick (Michigan Collection Rick) Most Collection Rick (Michigan Rick) Most Collection Rick (Mi
Rain Access (STREEDE)	On-view with fifting parameted, which we have been designed to be the foliation of the second or best force attacks of or best force attacks.	Data at Root	The control of t		r Low Low	Network	Нара	High	None	Unchanged	0.7	05 24	41	Low	62	36	password is provided then immediate changing the password is needed. Also ensure: 2. Statefull firewall 3. Do not store sensitive data in plaint	28 I. How to be closed before DR. 8 2. DIM DOMESTED 5-1.1 Malmost Description, Proceedings of the Conference of the Con	Report D001020164 DSTC001: GSL-STC-90 I	Low Low Low	r Network	Нідь	High Non	e Unchanged	0.7	0.5 1	4 41	3.6	Paths branch acceptable incer Stand-Madelling (2004) 1991-1991. See the control of the recordant of their first Cities State (Steel), High Risk (ed.) Opposite or in the Medium Risk (primary) regions. However, the individual risks were evaluated and reduced the ARAP to resume the extends and minigration are adequately evaluated to the extends and minigration are adequately evaluated to the extends and reduced to ARAP to extend the extends and extends and extends to ARAP to extend the extends and extends and extends the extends and extends and extends the extends of the extends and extend
Data Access (STR[I]DE)	Devices with default passwords which the default passwords which the default passwords which the default passwords which the default d	Authentication/Authorisation authorisation authorisation authorisation/()/app	1) Allowing application or origin to perform abnormal activities on the system. The property of the data, temporing the confidential data making it associated to the making it associated or the confidential data making it associated or confidential data making it associated or confidential in authorization/authorization data (overland) pane/1414, demonstracy or confidential panel pa	NA Hig	h None None	Network:	Нұр	High	None	Unchanged	8.7	86 36	44	Moderate	ūs	40	password is provided then immediate changing the password is needed. Also ensure: 2. Statefull firewall 3. Do not store sensitive data in plaint	air 1. Have to be closed before DR-8 y 2 CMM 0001020115-11 Mahoure Destriction/Protection 1. SAD/SIDD 0001020099-A7 Security SSC 000102002-2-112/system sha man praised of in management ASAD/SIDD 0001020099-A7 Security SSC 000102002-2-112/system sha man praised of in management SSC 000102002-2-112/system sha man praised of in management security of the security of	Report D001020164 DSTC001: GSL-STC-91 I	Low None None	e Network	High	High Non	e Unchanged	0.7	0.2 1	.4 22	18	ficial is brough accognitible sities: SmartMedic. Also and thow restablished in the Grinzel Bink. Also and thow restablished in the Grinzel Bink. File of the Grinzel Bink. File of the Grinzel Bink. However, the individuals of the Swere evaluated and reduced as JAPAP or summer the controls and miligation are adequately restablished by Levels. Levels.
Data Access (STR(IJDE)	Devices with default pacewords needs to be checked for brusteforce attacks	Data in Transit All	Adamonia spilication or script to perform abnormal activities on the 19 perform abnormal activities on the 19 perform abnormal activities on the 19 performs and 19 performs activities or challenging the integrity of data. In administration of the 19 performs activities activi	NA Hig	h None None	Network	High	High	None	Unchanged	8.7	0.6 3.6	44	Low	62	38	password is provided then immediate changing the password is needed. Also ensure: 2. Statefull firewall 3 Do not store sensitive data in plaints	alt 1. Have to be closed before DR-8 9 2. SSM D001020115-13. Malware Driection(Production std. 2. SAD/SDD-D001020099-6.7 Security SIS D001020023-2.11.35ystem that more parient at in anonymined facilities. 4.SAB/SDD-D001020099-6.7 Security SSS D001020023-2.11.35ystem shall store parient in in anonymined facilities.	DSTC001: GSL-STC-92 I	Low None None	e Network	High	High Non	e Unchanged	0.7	0.2	.4 22	1.6	Bith is broady acceptable discs Smortheds. Sold 1003030115-1. does not have recorded risks in the Crisical Bits. (Hoeld High Bits (2004) region on the Medium Bits (Systom) region. However, the individual risks were evaluated and reduced to AFAP or ensure the controls and miligations are adequately evaluated to the control of the Crisical Bits of the Crisical Bits of the Levels. LOW
Data Access (STR(IJDE)	The password complexity or location waterships, Like week passwords and hardcoaled passwords and hardcoaled passwords.	Data at Rest	Allowing application or script to perform abnormal activities on the oppose. John Modifying the data, tamporing the confidential data making it is John Modifying the data, tamporing the confidential data making it is John Modifying the data in tamporing the confidential data in the data (revelocities) performation related to authorized polymerization data (revelocities) performation (part of performance).	NA Lov	r Low Low	Network	High	High	None	Unchanged	0.7	85 3.4	41	Low	62	36	Similar de la companya del companya del companya de la companya del co	IN 1. New to be closed before DR-d 2. SIS-D00120027-12.12 If no longish Close is supported by the company of the longish Close is supported by the company of the company o	ng id	Low Low Low	r Network	High	High None	e Unchanged	0.7	0.5 :	.4 41	3.6	Side is brough acceptable since SmartShedic does not have resident risks in the Oricia Bade (Lead) High Bade
Data Access STR[I]DE)	Unprotected external USB Port on the tablet/devices.	Tablet Resources - web cam, microphone, O'T devices, Removable ISST Tablet Application, Newwork interfaces (Bastoods, Wift)	Altowing application or script to perform abnormal activities on the vocation. Modifying the data, tamporing the certification of an analog if unavailable or challenging the integrity of data. Constitution of the control of the contr		e Low Low	Physical	High	High	None	Unchanged	0.2	8.4 2.5	v	Moderate	es	2.6	Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported the application Use hardened interfaces (n/w) &	by Application shall support the use of anti-malware mechanism 3 SSS D001020024-2-23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices).	Document #: D001020037 Security Penetration Test Report: D001020164 DSTC001: GSL-STC-96	None Low Low	r Physical	High	High Non	e Unchanged	0.2	0.4	.5 2.7	2.6	Bids is brough acceptable disco Stauersbede, does not have residual risks in the Critical Bids. (Buckton/Protection (Tad.) Bigh Bids (1987) regione or in the Medium Bids (protection/Protection Bids (Protection/Protection Bids) region. However, the individual risks were evaluated and reduced not ANAP or seasons the controls and self-reduced to ANAP or seasons the controls and reduced new residual risks to the As for an Possible Levels.
pen network port exploit TTP)	Unprosected network port(s) on network port(s) on network devices and connection points	Tablet OS/nativorit details & Tablet Application Tablet Application	1) Cupture your account's user ID and crochestals. 2) Ling the data of coline traffic accessed on your tablet or competer. In the way, they can maintain a date of the websites you meanly void. 2) Call can come to your competer, its networks and data. 4) Launch a spass or malware estack on your device.		e None Low	Network:	High	Low	None	Unchanged	1.6	62 14	n	Moderate	0.5	23	the application 4. Use hundered interfaces (n/w) &	4. SISS D001020024 - 2.17.2The Application shall provide secure tunned Communications channel and 1.50M D0012015 - 11 Mahoure Detections/Protection 2.SISS D001020024 - 2.17.2The physication shall support the use of anti-malureum exchanism 3. SISS D001020024 - 2.23.1 The Application shall have logs of tablet opplication and firmware Cimarthéed devices).	DSTC001: GSL-STC-97	None None Low	r Network	Ніў	Low Non	e Unchanged	1.6	0.2	.4 31	23	Bild is brough acropatable sizes Smortheder, does not have residual risks in the Orikical Bild. Discussion of the residual risks in the Orikical Bild. Discussion of the Policy Republic Conference on the Medium. Bild optionly regions: a risk before exclusion of the Republic Republic Conference on the Republic Republic Conference on the Republic Republic Conference on the
Open nsework port exploit TTP)	Unprotected network port(s) on network devices and connection points	AGS	11 Capture your account's user ID and evoduration. 22 Leag the data of contine traffic accessed on your tablet or computer. In this way, they can maintain a data of the websites you mostly violic, and plan attack from these websites. 33 Cain a cores to your computer, it is network and data. 43 Launch a quan or maintain a data.		e None Low	Network	High	Low	None	Unchanged	1.6	02 1.4	31	Moderate	ůS	23	OW SOM responsibility 1. Stateful firewall and using port security on fewall 2. Configure router wireless security options based on manufacture manual	Application shall provide secure tunted Communications channel 1. SOM D001020115-13. Malware Detection/Protection 2. SOM D001020115-10.2. Configuration settlings	Document #: D001020037 Security Penetration Test Report D001020164 DSTC001: GSL-STC-98	None None Low	r Network	High	Low Non	e Unchanged	1.6	0.2	4 31	23	Eiski is bready acceptable since SmartMedic ideas test have resulted risks in the Orional Biological Since State Wave resulted risks in the Orional Biological Since State Orional Page 100 to the Indial Since State Orional Sinc
pem network port exploit TP)	Unencrypted Network segment through out the information flow	Tablet OS/network details & Tablet Application A02	I) Capture your account's user ID and crodestalls. 2) Legis due that of collection terrificare costs on your tablest or compare. In this way, they can aniatinis a data or the websites you mostly visit, and plan actuals from these websites. 3) Gain access to your computer, its network and data. () lanced a quant or maleness stands on your dericin.		e None Low	Network:	High	Low	None	Unchanged	1.6	02 14	31	Moderate	05	23	Anti-virus with updated virus definitions Andit/System log capturing any abnormal activity identified/reported the application Use hurdened interfaces in/wi &	and J. SOM D001020115 - 13. Malware Detection/Protection 2-SRS D001020024 - 2.17.6The Application shall support the use of anti-malware mechanism 3. SRS D001020024 - 2.23.1 The Application shall have logs of tablet application and firmware (SmartMedic devices).	Document #: D001020037 Security Penetration Test Report D001020164 DSTC001: GSL-STC-99	None None Low	r Network	High	Low Non	e Unchanged	1.6	0.2	4 31	23	reduces the ensural relation the Ad for an Promisible Disk is browned accomplaint ensurant broken disks and there resulted in the Critical Rule. Sold 8001820115— disks not have resulted rinks in the Critical Rule. Debection/Protection Disk (pricelys) regions. Disk to the Additional Rule (Pricelys Rule) Timework, the individual rule wave evaluated and selected an APAP is resurred the controls and miligations are adequately excitabilised to reduce the overall rules to the Act for an Presible Levels.

ince SmartMedic sin the Critical Risk on or in the Medium 2. SOM DOD Detection/F des were evaluated sure the controls and some the controls and	s in the Critical Risk on or in the Medium as were evaluated sure the controls and	s in the Critical Risk on or in the Medium iks were evaluated sure the controls and established to	s in the Critical Risk on or in the Medium iks were evaluated sure the controls and	s in the Critical Risk on or in the Medium iks were evaluated sure the controls and established to	s in the Critical Risk on or in the Medium sks were evaluated	s in the Critical Risk on or in the Medium acs were evaluated sure the controls and established to		s in the Critical Risk on or in the Medium 2. SO confi	in the Critical Bisk. or in the Medical Bisk. or in the Medical Bisk. con in the Medical Bisk. be the As far as Possible inne SmartMedic in the Critical Bisk. can be the Critical Bisk. can be considered and established to the Medical Bisk. can be considered the As far as Possible	is in the Crossol Bask The Cross of the Cross of the Cross The Cross of the Cross of the Cross of the Cross The Cross of the Cross	is on the Critical Billion The Committee of the Committe
relational Security Risk Acceptability (view laborated by the Control of the Cont	Rick is bready acceptable sizes: Smorthed- does not have residual ricks in the Critical (Red.) Righ Rick (red) regions or in the Me Rick (red) region. However, the individual ricks were vessel and and reduced to AFAP to ensure the contro- mingations are adequately established to reduce the overall ricks to the Afa for an Po- Levik.	Bisk is heavely acceptable since SmartMeddene and have residual risks in the Critical (Red.) High Risk (and project or in the Me. She for the	Edit is brauchy acceptable diese SmartMed does not have vesidant intels in the Civilian (Bud.) High Bids (red) region on in the Me talk (yellow) region. However, the individual risks were evalua and reduced to AFAP we essure the control reduced to AFAP and the control reduced to AFAP and the second the control reduce the everall risks to the Art far as Po Levels.	Rick is broadly acceptable sizes SmarMed does not have resident fields in the Cital does not have resident fields in the Cital does not have resident fields in the Cital Rick (Smith) registered in the Smith Rick (Smith) registered resident field field in the Rick (Smith) registered resident field in the Rick (Smith) registered resident field field in the Rick (Smith) registered resident field field in the Al far as Potardon field (Smith) registered resident field	Bids is broady acceptable disco SmartMed does not have evoluted risks in the Critical (Bod.) High Bids (red) region or in the Me Bids (yellow) progion. However, the individual risks were evaluated and reduced to AFAP to ensure the control and reduced to AFAP to ensure the control management of the reduced to the reduce	Ride is breasdy acceptable since SmartMed- does not have evident risks in the Critical (Rod.) High Ride (red) region or in the Me Ride (yellow) region. However, the individual risks over evalua- ant reduced to ARPA to ensure the control minigations are adequately established to reduce the everall risks to the Ar far as Po- Levels.	one	Did it is broady accordable about Street Mode does not have recolated does in the Carliad (tool) High Tills (red) regions or the Mee. Rich (prilling) regions. However, the individual rich was were evalua- and reduced on APP or ensures the contra- cation, the reversal rich is to the Arie for all Po- Levels.	Sizik is brough acceptable sizes SteamMed does not have vestical risks in the Christian (Incl.). High Bild (red) regions or in the Med Red (red) regions or in the Med Red (red) regions or in the Med Red (red). High Risk (red) regions or in the Med Red (red). He were or calculated a red (red). He was a region of the Red (red) or red (red) or red (red) or red (red). He was a region of the Red (red) or red (red). He was a red (red) or red) or red). He was a red (red) or red) or red). He was a red (red) region or in the Med Red (red). High Risk (red) regions or in the Med Red (red). High Risk (red) regions or in the Med Red (red). High Risk (red) regions or in the Med Red (red). High Risk (red) regions or in the Med Red (red). High Risk (red) regions or in the Med Red (red). High Risk (red) regions or in the Med Red (red). High Risk (red) regions or in the Med Red (red). High Risk (red) regions or in the Med Red (red) red). High Risk (red) regions or in the Med Red (red) red). High Risk (red) regions or in the Med Red (red) red). High Risk (red) regions or in the Med Red (red) red) red).	Esiá la Versely acceptable since StruetMedices en Chave versident riche in the Critical (tod.) High Rick (vol.) region or in the Me has been been been been been been been bee	Sink is broady acceptable since StarePlade does not have resident risks as the Crizzal Risk (gridlen) project.
	34 L	29 L	29 L	29 L	29 L	28 L		29 L		28 L	28 L
	25 42	25 13	25 33	25 33	25 33		25 30			25 23	25 29
	0.4	0.4	0.4	0.4	0.4		0.4		0.4 2	0.4 2	0.4 2
	1 16	0.7	0.7	0.7	0.7		0.5		27	0.7	0.7
See Scope Unchanged	one Unchanged	one Unchamped	one Unchanged	one Unchanged	one Unchanged		Unchamped			one Uncharged	one Unchanged
Privileges Required In	Low	High	High	High	High		High		Нул	High	High I
	High	High	High	High	High		High		High	High	High High
Attack Vector Attack Vector None Low Network	Low Low Network	None Low Network	None Low Network	None Low Network	None Low Network		None Low Local	None Low Local		Note Low Nationals	None Low Notwork Low Low Adjusted Releases
Measures (Effectiveness) Insertation Testing Protocol cuming #: D001020037 curity Penetration Test poper D001020164 STC001: GSL-STC-102	curity Penetration Test sport: D001020164 STC001: GSL-STC-103	port: D001020164 STC001: GSL-STC-104	STC001: GSL-STC-105	STC001: GSL-STC-107	ocument #: D001020037 curity Penetration Test sport: D001020164 STC001: GSL-STC-108	netration Testing Protocol ocument #: D001020037	STC001: GSL-STC-112	port DISSISSION TOTAL TO	port DISSISSION TOTAL TO	port DISSISSION TOTAL TO	Internation Trading Protection Internation Trading Protection
tunnel Communications channel	S. SAD/SDD-D001020099-6:7 Security* 1. SOM D001020115 - 13. Malware Detection/Protection 2-SRS D001020024 - 2.17.6The Application shall support the use of anti-malware mechanism	2. SRS D001020097 - 2.1.2.6 The Application shall be validated by using an invisible captcha during login. 3. SRS D001020097 - 2.1.2.1.1 Invalid email or password, only 3 attempts left. SRS D001020023-2.1.2.1.1 Invalid hospital code, only 3 attempts left.		SRS D001020097 – 2.1.2.6 The Application shall be validated by using invisible captcha during login. SRS D001020097 – 2.1.2.1.1 Invalid email or password, only 3 attempts loft	The setup & configuration process of	1. NSA-SDD-D001020110-4-2-2-Azure	2. SOM D001020115 - 7.1. Access	2. DOM DODISOUS 1-7.1 Acres control policy and management 1. SLD/1906. DODISOUS 999-6. T SLD/1906. DODISOUS 999-6. T SLD/1906. DODISOUS 999-6. T SASK-SCHOP 1. SLD/1906. DODISOUS 999-6. T SASK-SCHOP 1. SLD/1906. SLD/1	2. SIM DOSIDERISTS -7.1 Across correct policy and management of the control policy and contr	2. SIMM DODIEGOSTIST-7-1. Across correct policy and management correct policy and management of the correct policy and management policy and the correct policy and	2. SIOM DODIEGOSTIS - 7.1 Across correct policy and management of the control policy and cont
Security Eich Control Measures 1. Use across trained communication across trained across control (read/month) across trained	1. Asset should be behind standed forevar 2. Asset views with appliant views definitions the standard view of the standard views definitions 1. Asset, Tryptom bay capturing any absence all activity absentiately reported by the standard conference (phys) of secure tunnel communications channel secure tunnel communications channel	I During the across providing if defaulty password is provided then immediately changing the password in needed. 2. Require multi-factor arthresis for a state of the Limitary [In the Action of the Control of the Control Limitary [In the Action of the Control Limitary [In the Control Limitary [In the Control Limitary	1 During the access providing if default password is provided than immediately password in provided than immediately also sensure 2. Require multi-factor archivestication 1. Limit archivestication affecting from 1. Limit archivestication archives from 1. Limit archivestication archives for 1. Limit archivestication archives for 1. Requirement for failed, baged, in 1. Limit provided failed, baged, in 1. Limit from the failed for the failed for 1. Send frystem lag. Maintain security (say (such as failed) reduction provided from the failed for 1. Limit from the f	V 1. Strong password strength practices in recommended for admin who app. commended for admin who app. 2. Links arthrotication attempts (new Limiting) 4. Admit/prima log. Maintain Access 4. Admit/prima log. Maintain Access 4. Admit/prima log. Maintain security logs (see has though randitation of the primary and the security logs (see has though randitation of the primary administration of the primary administration of the security at 4. Stronger authentication methods	S 1. Strong password strength practices in recommended in name 2. Require multi-factor archerolaterisation 3. Inside archerolaterisation strength (and 1. Inside archerolaterisation strength (and 1. A multi-fryshman (p. Malatinia Accurate lage (logia (Interrupted & Barbick) laged; though a compared to the strength of		using Service-Managed keys (provided for azure) 2. Proper way of network access control 3. Encryption for sensitive data in transit for ex: when files are moved to cloud storage, etc.	using Service-Managed keys (provided for azure) 2. Proper way of network access control 3. Encryption for sensitive data in transit for ex: when files are moved to cloud storage, etc. 4. Transfer over encrypted tunnel	using Environ-Managed Baye (provided for natural) year for familiary of affective Access content of Encryption for resolution data in transit for each of the content of th	sing Service-Managed Bay (provided for surer) In Encryption for investigate data in transit 1. Transfer over encryption dignared 1. Transfer over encryption dignared 1. Transfer over encryption dignared 2. Configure and supprade resolvents for the 2. Configure service that is reject any purchase with spoofast adulterance 2. Configure formation for the service data in the service of the service o	sing Service Managed Bay (provided to marry) 10 marry 11 Encyption for remotive decrease control of the service of the servi
Overall Rick Score Se	34	2.9	29	29	29		2.8	1	2.9	2.9 345 4.5 4.5	2.9 MI 4.5 MI 4.
Threat Event Initiation Score	0. S	ø.s	a .s	e s	0.5		0.S	85		65	85
Threat Event Inditation Moderate	Moderate	Moderate	Moderate	Moderate	Moderate		Moderate	Moderate Moderate		Moderate	Moderate Moderate
CVSS v1.9 Base Score	42	33	33	33	33		3.0	2.0		33	33
Impact Sub Score	25	25	25	25	25		25	25		25	25
SC Base	0.4	0.4	84	0.4	0.4		0.4	04			
Exploitability Sub Score	16	0.7	0.7	0.7	0.7		0.5		8.7	87	6.7 5.4
	e Unchanged	e Unchanged	e Unchanged	e Unchanged	e Unchanged		e Unchanged			e Unchanged	e Unchanged
vileges quired User In	Low N	High N	High N	High N	High N		High N	Mgh X	Tigh X	Tigh X	Nigh N
Re	High	High	High	High	High		Migh		High	High High	Наја Наја
Vector Attack Con	vork High	vork High	vork Higi	work High	vark High		cal Nagi		nos. High	each High	eork High
a Low Network	r Low Network	e Low Netword	e Love Network	e Low Network	e Low Network		e Love Local			s Low Network	t Low Network High Adjacent Net High Adjacent Net
Select Propagat Resident Propagat N/A) Norme Norme Norme	A None Lo	A Low Nos	A Love Nos	A Low Not	A Low Not	A	Low Nos	Later No.	A Lear No.	A Leav No	A Leav No
Inspect Description () Copton year account's user 10 and croduction. () Logitus a year account's user 10 and croduction. () and the date of collect traffic, account you war belief or comparie. () and the date of collect traffic, account you war belief or comparie. () and the way, they can maintain adde of the websitesy you mostly visit, and plate actually not those websites. () Collect account is your comparier, the network and disa.	() Coption a pair account's sour D and crackershish. () Log the data of collising traffic accessment on your tables or computer. In this way, they care maintains adds of the websites you mostly visit, and have a considerable and the selection of the collision and	An attacker may attempt to discover a weak credential by An attacker may attempt to discover a weak credential by An attacker may attempt to discover the one correct combination that weeks An attacker may attempt to discover the one correct combination that weeks	I) As attacker may attempt to discover a weak conducted by yolumatically trying every possible combination of fetters, numbers, and guideds until it discovers the one correct combination that works.	1) An attacker may attempt to discover a weak conduction by potentially young every possible continuation of feature, unather, and young a supplied continuation of feature, unather, and yould continue feature for our connect conduction that works. If youldn't continue feature feature connect conduction that works.	I) As attacker may attempt to discover a weak conducted by yotenedically trying every possible combination of fetters, numbers, and gymbols until it discovers the one correct combination that works.	An attacker may attempt to discover a weak encryption by systematically trying every possible combination of decryption key.		1) As attacker may attempt to discover a weak encryption by optimistically trying every possible combination of the cryption key.	yntematically trying every possible combination of decryption key. 1) This theoret may hanger digital or physical resources, it discretes may hanger digital or physical resources, it discretes and end points of the control of the	(1) The threat may hamper digital or physical resources, (1) The threat may hamper digital or physical resources, (2) He the user (myshproy) closely continued to absence, (3) He the user (myshproy) closely continued to deveload subsers, and among us parlorm actions that are dangerous. (3) This threat may hamper digital or physical resources, (4) A continued may hamper digital or physical resources, (6) A continued may hamper digital or physical resources, (6) A continued may hamper digital or physical resources, (6) A continued may hamper digital or physical resources, (6) A continued may hamper digital or physical resources, (6) A continued may hamper digital or physical resources, (6) A continued may be a continued by the continued makes, (8) A continued may be a continued and makes, (8) A continued may be a continued and makes, (8) A continued may be a continued and makes, (8) A continued may be a continued and makes, (8) A continued may be a continued and makes, (8) A continued may be a continued and makes, (8) A continued may be a continued and makes, (9) A continued may be a continued and makes, (9) A continued may be a continued and makes, (1) A continued may be a continued and makes, (1) A continued may be a continued and makes, (1) A continued may be a continued and makes, (2) A continued may be a continued and makes, (3) A continued may be a continued and makes, (4) A continued may be a continued and makes, (5) A continued may be a continued and makes, (6) A continued may be a continued and makes, (7) A continued may be a continued and makes, (8) A continued may be a continued and makes, (8) A continued may be a continued and makes, (9) A continued may be a continued and makes, (1) A continued may be a continued and makes, (1) A continued may be a continued and makes, (1) A continued may be a continued and makes, (1) A continued may be a continued and makes, (1) A continued may be a continued and makes, (1) A continued may be a continued and makes, (2) A continu	y parameter and the property possible combination of decryption key. 1) This there may hamper digital or physical resources, and activation and end poince. 1) of the survey of complexes of control of control of control and analysis of control of control of control and control of control of control of control and control of control of control and control of control of control and control of control and control of control and control of control and control a
Asset Data in Transit A10	Tablet OS/notwork details & Tablet Application A02	Smart medic app (Stryker Admi Web Application)	Smart medic app (Anure Portal Administrator)	Smart medic app (Stryker Admi Web Application)	Smart medic app (Anare Portal Administrator)	Data at Rest	A09	A09 Data in Transit A10	A10 Smart modic app (Stryker Admit Modication) Wob Application) A11	A10 Smart moder app (Stryker Admi Wol Application) A11 Interfaces/API Communication A67	A10 Smart moder app (Stryker Admi Work Application) A11 Interface/APT Communication A07 Smart moder app (Anne Portal Administrator) A12 Smart moder app (Anne Portal
Vulner abilities Unencrypted data in transit in all flowchannels	Insecure communications in networks (hospital)	Devices with dafault parameters associed to the checked for brusheld for brusheld for brusheld for attacks	Devices with default paseowerds needs to be checked for brusteforce attacks	The password complexity or location vulnerability. Like weak possion of the password as an hardcoded password as a hardcoded password as the password and hardcoded password as the password and the password as the password	The password complexity or tocation valuerability. Like weak passworth and hardroded passworth.	Weak Encryption Implementation in data at rest and in transit tactical and design wise	VIII	Weah Earry year, Implementation in data at rest and in transit tacted and design wite	Weak Easy years Implementation in data at real and its transit sectors and design wise Legacy system identification if any years Legacy system identification if any	Weak Encryption Implementation in data at rest and in transit taction and design with a second control of the	Weak Easy years Implementation in data at real and its transit sectors and design wise Legacy system identification if any years Legacy system identification if any
Threat Event(s) Open network port exploit (TTP)	network port exploit	e Amack 2)	rrce Amack 112)	e Attack (2)	e Attack 12)	force Attack C-112)		ate drove Attack.	IC-112)	gine ering	(C-112)

Revision: AB Form																																	
				Adverse Impact								Pre-Implementation of Secur	ty Controls					Security Cont	trols/Mitigations							Post-Impleme	ntation of Security	Controls					
ID#	Threat Event(s)	Vulnerabilities	Asset	Impact Description	Safety Impact (Risk ID# or N/A)	Integrity	Attack V	ector Attack Complexity	Privileges Required	User Interaction	Scope	Exploitability Sub Score	ISC Base Impact Sub Sco	e CVSS v3.0 Base Score	Threat Event Initiation	Threat Event Initiation Score	Overall Risk Score		ntation of Risk Control Measures	erification of Risk Control Measures (Effectiveness)	Integrity	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Scope Explo	sitability Sub Score	SC Base Impact : Score	CVSS v3.0 Base Score	Overall Risk Score	Security Risk Residual S	Security Risk Acceptability Re Justification SC	marks (Column added additionaly I M Reference
94 TO	Gaining Access [[S]TRID[E]]	Improper security (for ex., Storage & Access) for Key tokens and Certificates V30	Azure Cloud DataBase	1) An attaker may attempt to discover a weak credential by optionalized or districts, number and symbols until it discovers the one correct combination that we also specified by the optional properties of the optional properties	reks.	Low	High Netwo	rk High	Low	None	Unchanged	1.6	0.7 4.7	6.4	Moderate	0.5	5.6	keys/certificates, their generation & Cosmos DB storage should be done securely. 2. Apart from user id there should be	Doc Sec Rep e closed before DR-8	netration Testing Protocol cument #: D001020037 curity Penetration Test port: D001020164 TC001: GSL-STC-128	ione None	Low Network	High	Low	None	Unchanged	1.6	0.2 1.4	31	23	does not have (Red). High Ris Risk (yellow) r However, the is and reduced to mitigations are	acceptable since SmartMedic esidual riske in the Cristical Risk k [red] region or in the Medium egion. adividual risks were evaluated AFAP to ensure the controls and adequately established to rall risks to the As far as Possible	
95 TO	Gaining Access ([S]TRID(E])	Absence of additional security factor along with user identification	Smart medic app (Axure Portal Administrator)	1)An attacker may attempt to Goscover a weak credental by systematically trying every possible conditions of textres, unabless and symbols until it discovers the one current combination that was and symbols until it discovers the one current combination that was the condition of the combination of the combinatio	or Res.	Low	High Netwo	rk High	Low	None	Unchanged	1.6	67 47	6.4	Moderate	0.5	5.6	MERCIN. 1. Have point on the accessed by logis properties of the stemp & company password policies & management are required. 2. It disturbes access using lawy contribution, the company contribution is a properties of the company contribution, their generation & 1. Apart from some in them should be additional accessify factor for verification. 4. Limit on the logia attempts is mandatury, a management of the contribution	& admin shall be If and published within the In for the corresponding If the admin portal	current #: D001020037 curity Penetration Test port: D001020164	ione None	Low Network	High	Low	None	Unchanged	1.6	0.2 1.4	31	23	does not have a (Red). High Ris Risk (yellow) a LOW However, how and reduced to mitigations are	acceptable since SmartMedic esidual risks in the Crisical Risk (a (red) region or in the Medium agion. divisidual risks were evaluated AFAP to ensure the controls and adequately established to rall risks to the As far as Possible	
96 TO	Gaining Access ([S]TRID(E])	Absence of additional security factor along with user identification V25	Azure Goud DataBase	1.) An attacker may attempt to discover a weak conductal by optional collaboration of the conductal by optional collaboration of the conductal conductation of the conductation of th	erks.	Low	High Netwo	rk High	Low	None	Unchanged	1.6	0.7 4.7	6.4	Moderate	0.5	5.6	(keys/certificates) for verification. Cosmos DB	Doi Sec Rep 01020031 - 2.2.1.7 -	netration Testing Protocol cument #: D001020037 cumity Penetration Test port: D001020164 TC001: GSL-STC-128	ione None	Low Network	High	Low	None	Unchanged	1.6	0.2 1.4	31	23	does not have a (Red). High Ris (Red). High Ris (Red). High Ris (Red). However, the is and reduced to mitigations are	acceptable since SmartMedic esidual risks in the Cristcal Risk k [red] region or in the Medium agion. adividual risks were evaluated AFAP to ensure the controls and adequately established to rall risks to the As far as Possible	
97 T1	Brute-force Attack (CAPEC-112)	Error Info containing sensitive data for Failed Authentication attempts	Azure Cloud DataBase	1) An attacker may attempt to discover a weak credential by optional collaboration of the control of the c	refes.	Low	High Netwo	rk High	Low	None	Unchanged	1.6	0.7 4.7	6.4	Moderate	0.5	5.6	Apart from user if there should be additional security factor for verification. Limit on the login attempts is mandatory. Cosmos DB	ould be displayed upon f credentials to mitigate count harvesting and n. DST D1020031 - 2.2.1.7 -	current #: D001020037 currity Penetration Test port: D001020164	ione None	Low Network	High	Low	None	Unchanged	1.6	0.2 1.4	31	23	does not have a (Red). High Ris Risk (yellow) a However, the is and reduced to mitigations are	acceptable since SmartMedic esidual riske in the Critical Risk k (red) region or in the Medium egion. adividual risks were evaluated AFAP to ensure the controls and adequately established to rall risks to the As far as Possible	
98 T1	Brute-force Attack (CAPEC-112)	Having no limit on the login attempts		John attader may attempt to Geovera weak credental by systematically trying ever possible consistance of terres, resulta- zated symbols until it discovers the one correct combination that wor and symbols until it discovers the one correct combination that wor	refes.	Low	High Netwo	rk High	Low	None	Unchanged	1.6	07 47	6.4	Moderate	0.5	5.6	2. Apart from user if there should be additional security factor for verification. 3. Limit on the login attempts is 2.5 Ab DO Cosmos IB 3. The strup of zarrer close.	ud & admin shall be J and published within the In for the corresponding the admin portal DIST 01020031 - 2.2.1.7 - 0.8 configuration process ud & admin shall be	cument #: D001020037 curity Penetration Test port: D001020164	ione None	Low Network	High	Low	None	Unchanged	1.6	0.2 1.4	3.1	23	does not have a (Red). High Ris Risk (yellow) a LOW However, the and reduced to mitigations are	-	
99 T1	Unauthorized Alterations (S[T]RIDE)	Improper/insufficient provisioning of IOT hub		I. If provincing get haled/minds aded then the complete functions are stillened. The provincing the provincing failure needs to addressed. Proper reason for the provisioning failure needs to addressed.	1	None I	High Netwo	rk High	High	None	Unchanged	0.7	06 36	44	Low	0.2	3.8	LOW 1. If devices which need to be registered Flow to be of the control of the co	Dor Sec Reg DST	netration Testing Protocol cument 8: D001020037 curity Penetration Test port D001020164 TC001: GSL-STC-37 TC001: GSL-STC-71 TC001: GSL-STC-79	ione None	Low Network	High	High	None	Unchanged	0.7	0.2 1.4	22	16	does not have a (Red). High Ris Risk (yellow) a LOW However, how and reduced to mitigations are	acceptable since SmartMedic estidual riske in the Critical Risk (E (red) region or in the Medium agion. adividual risks were evaluated AFAP to ensure the controls and adequately established to rall risks to the As far as Possible	
100 T:	Unauthorized Alterations (S[T]RIDE)	Unsecured communication with unauthenticated 3rd party devices V32	Tablet OS/notwork details & Tablet Application	If there is uperpayer endourtections between the devices in the sou- mentic envelopment than 5th party province can easily variabilish the communication with the strylers devices		None i	High Netwo	rk High	High	None	Unchanged	0.7	06 36	44	Low	0.2	3.8	2. Secure communication between the strylear devices needs to be established if she did documented 3. Hamfung of the unaushericated 3rd party devices trying to communicate with strylear devices needs to be taken	Document of the communicate with and tablet. Document of the communicate with and tablet. DISTRUCTOR OF THE CONTRACT OF T	cument #: D001020037 currly Penetration Test port: D001020164 TC001: GSL-STC-37	ione None	Low Network	High	High	None	Unchanged	0.7	0.2 1.4	22	16	does not have a (Red). High Ris Risk (yellow) a However, the LOW	acceptable since SmartMedic usidaul risks in the Critical Risks (k red) region or in the Medium agion. Maintenance of the Medium agion. Maintenance of the Medium dividual risks were evaluated AFAP to ensure the controls and adequately established to call risks to the As far as Possible	

Doc Number: D000000909 Name: Product Security Risk Table Revision: AB Form

Security Risk Assessment Summary

ID#		Threat Event(s)		Vulnerabilities		Assets	Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
5		Deliver undirected malware (CAPEC-185)	V22	Legacy system identification if any	A03	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
6	T01	Deliver undirected malware (CAPEC-185)	V22	Legacy system identification if any	A01	Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
7	T01	Deliver undirected malware (CAPEC-185)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A05	Device Maintainence tool (Hardware/Software)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
8	T01	Deliver undirected malware (CAPEC-185)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
9	T01	Deliver undirected malware (CAPEC-185)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A03	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible

Stryker Confidential Page 13 of 29

Doc Number: D000000909 Name: Product Security Risk Table Revision: AB

Form									n a		D . 2	
ID#		Threat Event(s)		Vulnerabilities		Assets	Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
10	T01	Deliver undirected malware (CAPEC-185)		Software Vulnerability Management			1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
11	T01	Deliver undirected malware (CAPEC-185)	V09	Lack of plan for periodic Software Vulnerability Management	A01	Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
12	T01	Deliver undirected malware (CAPEC-185)	V09	Lack of plan for periodic Software Vulnerability Management	A03	Smart medic (Stryker device) System Component	Malicious utilization of computer resources 2) computing power denial of service attacks, ransomware attack Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
13	T01	Deliver undirected malware (CAPEC-185)	V12	Unprotected network port(s) on network devices and connection points	A01	Application, Network interfaces (Bluetooth, Wifi)	Malicious utilization of computer resources computing power denial of service attacks, ransomware attack Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
14	T01	Deliver undirected malware (CAPEC-185)	V12	Unprotected network port(s) on network devices and connection points	A03		1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible

Stryker Confidential Page 14 of 29

Doc Number: D000000999 Name: Product Security Risk Table Revision: AB

Form												
ID#		Threat Event(s)		Vulnerabilities		Assets	Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
15		Deliver undirected malware (CAPEC-185)		Unencrypted data at rest in all possible locations		Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	Malicious utilization of computer resources computing power denial of service attacks, ransomware attack Bitcoin mining, etc	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
16	T01	Deliver undirected malware (CAPEC-185)		Unencrypted data in transit in all flowchannels	A03	System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
17	T01	Deliver undirected malware (CAPEC-185)	V17	Unencrypted data in transit in all flowchannels	A01	microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
18	T01	Deliver undirected malware (CAPEC-185)		Outdated - Software/Hardware	A05	(Hardware/Software)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
19	T01	Deliver undirected malware (CAPEC-185)		Outdated - Software/Hardware	A03	System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible

Stryker Confidential Page 15 of 29

Doc Number: D000000999 Name: Product Security Risk Table Revision: AB

orm								C-C-LI	Dw. C. 1		Dogt Cart 1	Decidual Committee District
ID#		Threat Event(s)		Vulnerabilities		Assets	Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
20	T01	Deliver undirected malware (CAPEC-185)	V23	Outdated - Software/Hardware	A01	Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
21	T02	Deliver directed malware (CAPEC-185)	V21	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	A05		1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
22	T02	Deliver directed malware (CAPEC-185)	V21	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	A03	Smart medic (Stryker device) System Component	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
23	T02	Deliver directed malware (CAPEC-185)	V21	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	A01	Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
24	T02	Deliver directed malware (CAPEC-185)	V13	Unprotected external USB Port on the tablet/devices.	A08		1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	SOM responsibility 1. Statefull Firewall 2. Maintain access control (read/modify) permission list for any sensitive & unencrypted data if present.	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible

Stryker Confidential Page 16 of 29

Doc Number: D000000999 Name: Product Security Risk Table Revision: AB

ID#		Threat Event(s)		Vulnerabilities		Assets	Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
25	Т02	Deliver directed malware (CAPEC-185)	V13	Unprotected external USB Port on the tablet/devices.	A01	Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
26	T02	Deliver directed malware (CAPEC-185)	V13	Unprotected external USB Port on the tablet/devices.	A11		1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
27	T02	Deliver directed malware (CAPEC-185)	V02	External communications and exposure for communciation channels from and to application and devices like tablet and smartmedic device.	A01	Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	MEDIUM	Only stryker made/authenticated devices should communicate with smart medic device & tablet Asset should be behind stateful firewall Use secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
28	T02	Deliver directed malware (CAPEC-185)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A05		1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
29	Т02	Deliver directed malware (CAPEC-185)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A03		1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible

Stryker Confidential Page 17 of 29

Doc Number: D000000999 Name: Product Security Risk Table Revision: AB

Form												
ID#		Threat Event(s)		Vulnerabilities		Assets	Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
30	T02	Deliver directed malware (CAPEC-185)	V08	Ineffective patch management of firware, OS and applications thoughout the information system plan	A01	Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
31	T02	Deliver directed malware (CAPEC-185)	V12	Unprotected network port(s) on network devices and connection points	A03		1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	MEDIUM	Only Stryker/HDO authenticated devices should communicate with smart medic device & tablet Asset should be behind stateful firewall Use secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
32	T02	Deliver directed malware (CAPEC-185)	V12	Unprotected network port(s) on network devices and connection points	A01	Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
33	T02	Deliver directed malware (CAPEC-185)	V21	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	A11	Web Application)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Deployed (V&V) secure system configuration model needs to be mentioned in the installation manual. 2. Establish internal and external information sources for threat intelligence and vulnerability data, monitoring them regularly and taking appropriate action for high-priority items 3. Use upgraded software, firmware 4. Never create/use credentials with personal details such as date of birth, spouse, or child's or pet's name 5. Stateful Firewall	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible Levels.
34	T02	Deliver directed malware (CAPEC-185)	V21	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	A01	Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	Low	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible

Stryker Confidential Page 18 of 29

Doc Number: D000000999 Name: Product Security Risk Table Revision: AB

Form												
ID#		Threat Event(s)		Vulnerabilities		Assets	Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
35	T02	Deliver directed malware (CAPEC-185)	V16	Unencrypted data at rest in all possible locations	A01	Application, Network interfaces (Bluetooth, Wifi)	1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
36	T02	Deliver directed malware (CAPEC-185)	V16	Unencrypted data at rest in all possible locations	A02		1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
37	T02	Deliver directed malware (CAPEC-185)	V16	Unencrypted data at rest in all possible locations	A11		1) Malicious utilization of computer resources 2) computing power 3) denial of service attacks, 4) ransomware attack 5) Bitcoin mining, etc	NA	LOW	1. Identification of the sensitive data in storage and encryption of storage subsystem 2. Stateful firewall 3. Hardening of the host system containing sensitive data at rest 4. Maintain access control (read/modify) permission list for any sensitive & unencrypted data if present. 5. Use strong encryption algorithm	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
38	Т03	Gaining Access ([S]TRID[E])	V12	Unprotected network port(s) on network devices and connection points	A02		Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerabilities.	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
39	Т03	Gaining Access ([S]TRID[E])	V12	Unprotected network port(s) on network devices and connection points	A11	Web Application)	Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerabilities.	NA	MEDIUM	1. Admin application can be accessed by login credentials & MFA. Hence, strong password policies & management are required 2. Data transfer between the admin application and the smart medic components needs to be encrypted & secured. 3. Any vulnerable network ports and connection points should be identified and hardened. 4. Maintain access control (read/modify) permission list for any sensitive & unencrypted data if present. 5. Stateful firewall	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible Levels.

Stryker Confidential Page 19 of 29

Doc Number: D000000999 Name: Product Security Risk Table Revision: AB

Form

Form					<u> </u>		_				
ID#	Threat Event(s)		Vulnerabilities		Assets	Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
40	T03 Gaining Access ([S]TRID[E])	V12	Unprotected network port(s) on network devices and connection points	A01	Application, Network interfaces (Bluetooth, Wifi)	Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerabilities.	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
41	T03 Gaining Access ([S]TRID[E])	V01	Devices with default passwords needs to be checked for bruteforce attacks	A04	Authentication/Authorisation method of all device(s)/app	Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerabilities.	NA	MEDIUM	1.During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: 2. Require multi-factor authentication 3. Limit authentication attempts (rate Limiting) 4. Maintain Access Logs	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
42	T03 Gaining Access ([S]TRID[E])	V01	Devices with default passwords needs to be checked for bruteforce attacks	A07	Interface/API Communication	Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerabilities.	NA	LOW	1. During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: 2. Require multi-factor authentication 3. Limit authentication attempts (rate Limiting) 4. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 5. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.) 6. Stronger authentication methods	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible Levels.
43	T03 Gaining Access ([S]TRID[E])	V03	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	A04		Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerabilities.	NA	MEDIUM	1. If devices/apps being accessed by login credentials & MFA. Then, strong password policies & management are required 2. Require multi-factor authentication 3 Limit authentication attempts (rate Limiting) 4. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 5. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.) 6. Stronger authentication methods	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible Levels.

Stryker Confidential Page 20 of 29

Doc Number: D000000909 Name: Product Security Risk Table Revision: AB

Form								1				
ID#		Threat Event(s)		Vulnerabilities		Assets	Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
44	Т03	Gaining Access ([S]TRID[E])	V04	Checking authentication modes for possible hacks and bypasses	A04	Authentication/Authorisation method of all device(s)/app	Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerabilities.	NA	LOW	Encrypt the authentication data in storage & transit to mitigate risk of information disclosure and authentication protocol attacks Encrypt authentication data using non reversible encryption such as using a digest (e.g., HASH) and a seed to prevent dictionary attacks Lock out accounts after reaching a log on failure threshold and mitigate risk of brute force attacks Display generic error messages upon validation of credentials to mitigate risk of account harvesting or enumeration	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible Levels.
45	Т03	Gaining Access ([S]TRID[E])	V04	Checking authentication modes for possible hacks and bypasses	A11		Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerabilities.	NA	LOW	Encrypt the authentication data in storage & transit to mitigate risk of information disclosure and authentication protocol attacks Encrypt authentication data using non reversible encryption such as using a digest (e.g., HASH) and a seed to prevent dictionary attacks Lock out accounts after reaching a log on failure threshold and mitigate risk of brute force attacks Display generic error messages upon validation of credentials to mitigate risk of account harvesting or enumeration	Low	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible Levels.
46	Т03	Gaining Access ([S]TRID[E])	V04	Checking authentication modes for possible hacks and bypasses	A12	Smart medic app (Azure Portal Administrator)	Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerabilities.	NA	LOW	Encrypt the authentication data in storage & transit to mitigate risk of information disclosure and authentication protocol attacks Encrypt authentication data using non reversible encryption such as using a digest (e.g., HASH) and a seed to prevent dictionary attacks Lock out accounts after reaching a log on failure threshold and mitigate risk of brute force attacks Display generic error messages upon validation of credentials to mitigate risk of account harvesting or enumeration	Low	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible Levels.
47	Т03	Gaining Access ([S]TRID[E])	V13	Unprotected external USB Port on the tablet/devices.	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerabilities.	NA	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible

Stryker Confidential Page 21 of 29

Doc Number: D000000999 Name: Product Security Risk Table Revision: AB

Form

Form								1	_			
ID#		Threat Event(s)		Vulnerabilities		Assets	Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
48	T04	Maintaining Access (TTP)	V01	Devices with default passwords needs to be checked for bruteforce attacks	A04	Authentication/Authorisation method of all device(s)/app	Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerabilities.	NA	LOW	1. During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: 2. Require multi-factor authentication 3. Limit authentication attempts (rate Limiting) 4. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 5. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.) 6. Stronger authentication methods	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible Levels.
49	Т04	Maintaining Access (TTP)	V03	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	A04	Authentication/Authorisation method of all device(s)/app	Obtain knowledge about system internals Attempt to find attack vectors Possibilities for exploitation of publicly known Vulnerabilities.	NA	LOW	1. If devices/apps being accessed by login credentials & MFA. Then, strong password policies & management are required 2. Require multi-factor authentication 3. Limit authentication attempts (rate Limiting) 4. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 5. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.) 6. Stronger authentication methods	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible Levels.
50	T05	Clearing Track (TTP)		InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	Tampering of forensic data This involves modifying/corrupting/deleting the values of Logs, Modifying registry values Uninstalling all malcious applications/tools Deleting all folders which were created	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
51		(ТТР)		Outdated - Software/Hardware	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malcious applications/tools 5) Deleting all folders which were created			1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
52	T05	Clearing Track (TTP)		Lack of configuration controls for IT assets in the informaion system plan	A01	Tablet Resources - web cam, microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malcious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table an	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible

Stryker Confidential Page 22 of 29

Doc Number: D000000999 Name: Product Security Risk Table Revision: AB

D #		Threat Event(s)	Vulnerabilities		Assets	Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
53	T05	Clearing Track (TTP)	Lack of configuration controls for IT assets in the informaion system plan	A05	(Hardware/Software)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malcious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table and		1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel		Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
54	T05	Clearing Track (TTP)	Ineffective patch management of firware, OS and applications thoughout the information system plan	A01	Application, Network interfaces (Bluetooth, Wifi)	1) Tampering of forensic data 2) This involves modifying/corrupting/deleting the values of Logs, 3) Modifying registry values 4) Uninstalling all malcious applications/tools 5) Deleting all folders which were created	B-L2(Reference Risk Table and	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
55	T05	Clearing Track (TTP)	Ineffective patch management of firware, OS and applications thoughout the information system plan	A05		Tampering of forensic data This involves modifying/corrupting/deleting the values of Logs, Modifying registry values Uninstalling all malcious applications/tools Deleting all folders which were created	B-L2(Reference Risk Table and	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
56	T05	Clearing Track (TTP)	Ineffective patch management of firware, OS and applications thoughout the information system plan	A02		Tampering of forensic data This involves modifying/corrupting/deleting the values of Logs, Modifying registry values Uninstalling all malcious applications/tools Deleting all folders which were created	B-L2(Reference Risk Table and	LOW	1. Asset should be behind stateful firewall 2. Anti-virus with updated virus definitions 3. Audit/System log capturing any abnormal activity identified/reported by the application 4. Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
57	T05	Clearing Track (TTP)	The static connection digaram between devices and applications with provision for periodic updation as per changes	A05		Tampering of forensic data This involves modifying/corrupting/deleting the values of Logs, Modifying registry values Uninstalling all malcious applications/tools Deleting all folders which were created	B-L2(Reference Risk Table and	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible

Stryker Confidential Page 23 of 29

Doc Number: D000000999 Name: Product Security Risk Table Revision: AB

Form									Part Controls			
ID#		Threat Event(s)		Vulnerabilities		Assets	Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
58	Т05	Clearing Track (TTP)		The static connection digaram between devices and applications with provision for periodic updation as per changes	A01	microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	Tampering of forensic data This involves modifying/corrupting/deleting the values of Logs, Modifying registry values Uninstalling all malcious applications/tools Deleting all folders which were created	B-L2(Reference Risk Table and	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
59	T06	Elevation of privilege (STRID[E])		Controlled Use of Administrative Privileges over the network	A04		Gaining access to the portal Accessing confidential data, Lead misuse of confidential data Company defamation	NA	LOW	Require that administrators establish multi factor authentication for their administrator and non-administrative accounts. Access to a machine (either remotely or locally) should be blocked for administrator-level accounts. Ensure default credentials not existing for any assets (such as applications, operating systems, routers, firewalls, wireless access points).	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible Levels.
60	T06	Elevation of privilege (STRID[E])	V15	Controlled Use of Administrative Privileges over the network	A12		Gaining access to the portal Accessing confidential data, Lead misuse of confidential data Company defamation	NA	MEDIUM	Require that administrators establish multi factor authentication for their administrator and non-administrative accounts. Access to a machine (either remotely or locally) should be blocked for administrator-level accounts. Ensure default credentials not existing for any assets (such as applications, operating systems, routers, firewalls, wireless access points).	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible Levels.
61	T07	Denial of service (STRI(D)E)		Unprotected network port(s) on network devices and connection points	A02	Tablet OS/network details & Tablet Application	Bring down the service availability Blocking the end user usage	NA	MEDIUM	Asset should be behind stateful firewall Anti-virus with updated virus definitions System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
62	T08	Information disclosure (STR(I)DE)		Unencrypted data at rest in all possible locations	A09		Information of health data can be exploit and disclose with various means like network, tablet etc	NA	LOW	1. Identification of the sensitive data in storage and encryption of storage subsystem 2. Stateful firewall 3. Hardening of the host system containing sensitive data at rest 4. Maintain access control (read/modify) permission list for any sensitive & unencrypted data if present. 5. Use strong encrption algorithm	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible

Stryker Confidential Page 24 of 29

Doc Number: D000000909 Name: Product Security Risk Table Revision: AB

Form I							Safety Impact	Dro Control		Post Control	Pacidual Cognitive Diale Assautability
ID#	Threat Event(s)		Vulnerabilities		Assets	Impact Description	(Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
63	TO8 Information disclosure (STR(I)DE)		Unencrypted data in transit in all flowchannels	A10	Data in Transit	Information of health data can be exploit and disclose with various means like network, tablet etc	NA	LOW	1. Use secure tunnel communication channel 2. Configure and upgrade routers for the n/w security 3. Configure firewalls to reject any packets with spoofed addresses. 4. Maintain access control (read/modify) permission list for any sensitive & unencrypted data if present. 5. For sensitive data proper encryption mechanism needs to be designed & implemented	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible Levels.
	T08 Information disclosure (STR(I)DE)		Weak Encryption Implementaion in data at rest and in transit tactical and design wise		Data at Rest	Information of health data can be exploit and disclose with various means like network, tablet etc	NA	LOW	Implement server-side encryption using Service-Managed keys/recomended practise by azure. Proper way of network access control 3. Encryption for sensitive data in transit, for ex: when files are moved to cloud storage, etc Transfer over encrypted tunnel 5. Use strong encryption algorithm	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
65	T08 Information disclosure (STR(I)DE)	V18	Weak Encryption Implementaion in data at rest and in transit tactical and design wise	A10	Data in Transit	Information of health data can be exploit and disclose with various means like network, tablet etc	NA	LOW	1. Statefull firewall 2. Configure and upgrade routers for the n/w security 3. Configure firewalls to reject any packets with spoofed addresses. 4. Use secure tunnel communication channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
66	T08 Information disclosure (STR(I)DE)		Weak Algorthim implementation with respect cipher key size	A09	Data at Rest	Information of health data can be exploit and disclose with various means like network, tablet etc	NA	LOW	Weak algorithms such as DES, RC4, etc should be avoided and usage of strong algorithms such as AES, RSA, etc are recomended Typical key lengths are 128 and 256 bits for private keys and 2048 for public keys are recommended.	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
67	T08 Information disclosure (STR(I)DE)	V19	Weak Algorthim implementation with respect cipher key size	A10	Data in Transit	Information of health data can be exploit and disclose with various means like network, tablet etc	NA	LOW	Weak algorithms such as DES, RC4, etc should be avoided and usage of strong algorithms such as AES, RSA, etc are recomended Typical key lengths are 128 and 256 bits for private keys and 2048 for public keys are recommended.	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible

Stryker Confidential Page 25 of 29

Doc Number: D000000999 Name: Product Security Risk Table Revision: AB

Form											
ID#		Threat Event(s)	Vulnerabilities		Assets	Impact Description	Safety Impact (Risk ID# or N/A)	Pre-Controls Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
68	T08	(STR(I)DE)	InSecure Configuration for Software/OS on Mobile Devices, Laptops, Workstations, and Servers	A01	microphone, OTG devices, Removable USB, Tablet Application, Network interfaces (Bluetooth, Wifi)	Information of health data can be exploit and disclose with various means like network, tablet etc	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel		Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
69	T08	Information disclosure (STR(I)DE)	Unencrypted Network segment through out the information flow	A10		Information of health data can be exploit and disclose with various means like network, tablet etc	NA	LOW	1. Anonymization/Pseudomyzation of patient details 2. Data encyrption 3. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 4. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.)	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
70	T08	Information disclosure (STR(I)DE)	Insecure communications in networks (hospital)	A10		Information of health data can be exploit and disclose with various means like network, tablet etc	NA	LOW	Secure communication with Secure Sockets Layer (SSL) or TLS protocols that provide message confidentiality Secure sensitive data in the channel flow using strong encryption Statefull firewall Proper way of network access control	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
71		(STR[I]DE)	Unprotected network port(s) on network devices and connection points	A01	microphone, OTG devices,	Allowing application or script to perform abnormal activites on the system. Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data.	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible
72	Т09	Data Access (STR[I]DE)	Unprotected network port(s) on network devices and connection points	A02		Allowing application or script to perform abnormal activites on the system. Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data.	NA	LOW	Asset should be behind stateful firewall Anti-virus with updated virus definitions Audit/System log capturing any abnormal activity identified/reported by the application Use hardened interfaces (n/w) & secure tunnel communications channel	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible

Stryker Confidential Page 26 of 29

Doc Number: D000000999 Name: Product Security Risk Table Revision: AB

Form

Form											
ID#	Threat Event(s)		Vulnerabilities		Assets	Impact Description	Safety Impact (Risk ID# or N/	A) Risk Level	Security Risk Control Measures	Post-Controls Risk Level	Residual Security Risk Acceptability Justification
	(STR[I]DE)	V01	Devices with default passwords needs to be checked for bruteforce attacks	A09	Data at Rest	Allowing application or script to perform abnormal activites on the system. Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data.		LOW	During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: Statefull firewall Do not store sensitive data in plaintext. Use strong encrption algorithm. Apply salting over sensitive data.	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible Levels.
74	T09 Data Access (STR[I]DE)	V01	Devices with default passwords needs to be checked for bruteforce attacks	A04	Authentication/Authorisation method of all device(s)/app	Allowing application or script to perform abnormal activites on the system. Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data. Information related to authenication/authorisation data (credential/pins/MFA/Biometrics)	NA	MEDIUM	During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: Statefull firewall Do not store sensitive data in plaintext. Use strong encrption algorithm. Apply salting over sensitive data.	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible Levels.
75	T09 Data Access (STR[I]DE)	V01	Devices with default passwords needs to be checked for bruteforce attacks	A10	Data in Transit	Allowing application or script to perform abnormal activites on the system. Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data. Information related to authenication/authorisation data (credential/pins/MFA/Biometrics)	NA	LOW	During the access providing, if default password is provided then immediately changing the password is needed. Also ensure: Statefull firewall Do not store sensitive data in plaintext. Use strong encrption algorithm. Apply salting over sensitive data.	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible Levels.
76	T09 Data Access (STR[I]DE)	V03	The password complexity or location vulnerability. Like weak passwords and hardcoded passwords.	A09		Allowing application or script to perform abnormal activites on the system. Modifying the data, tampering the confidential data making it unavailable or challenging the integrity of data. Information related to authenication/authorisation data (credential/pins/MFA/Biometrics)	NA	LOW	Strong password strength practices is recommended for admin web app. Require multi-factor authentication Limit authentication attempts (rate Limiting) 4. Audit/System log - Maintain Access logs (login (attempted & failed), logoff, id change) 5. Audit/System log - Maintain security logs (such as change/modification of system configuration settings, services, etc.) 6. Stronger authentication methods	LOW	Risk is broady acceptable since SmartMedic does not have residual risks in the Critical Risk (Red). High Risk (red) region or in the Medium Risk (yellow) region. However, the individual risks were evaluated and reduced to AFAP to ensure the controls and mitigations are adequately established to reduce the overall risks to the As far as Possible Levels.
		\vdash									
		\vdash									

Printed copies for reference only

Stryker Confidential - This document contains information that is confidential and proprietary. Neither this document nor the information herein may be reproduced, used, or disclosed to or for the benefit of any third party without the prior written consent of Stryker.

Stryker Confidential Page 27 of 29

Doc Number: D000000909 Name: Product Security Risk Table

Revision: AB Form

Common Vulnerability Scoring System (CVSS v3.0)

Exploitability Metrics												
Attack '	Vector		Attack Complexity			Privelege Required				User Interaction		
Metric	Metric	Value	Code	Metric	Value		Code	Metric	Value	Code		
Network	0.85	N	Low	0.77	L	None	0.85	0.85	N	None	0.85	N
Adjacent Network	0.62	A	High	0.44	Н	Low	0.62	0.68	L	Required	0.62	R
Local	0.55	L				High	0.27	0.5	Н			
Physical	0.2	P										

	Technical Impact Metrics										
Confidentiality	Confidentiality, Integrity, Availability Impact										
Metric	Metric Value Code										
None	0	N	$ISC_{Base} = 1 - [(1-Impact_{Conf}) \times (1-Impact_{Integ}) \times (1-Impact_{Avail})]$								
Low	0.22	L									
High	0.56	Н									

	Scope	
Unchanged	An exploited vulnerability can only affect resources managed by the same authority. In this case the vulnerable component and the impacted component are the same.	U
Changed	An exploited vulnerability can affect resources beyond the authorization privileges intended by the vulnerable component. In this case the vulnerable component and the impacted component are different.	С

ASSUMPTIONS:

Base metrics

For the purposes of the medical device only Base metrics are considered. The Base metric group represents the intrinsic characteristics of a vulnerability that are constant over time and across user environments. It is composed of two sets of metrics: the Exploitability metrics and the Impact metrics.

The Exploitability metrics reflect the ease and technical means by which the vulnerability can be exploited. That is, they represent characteristics of the thing that is vulnerable, which we refer to formally as the vulnerable component. On the other hand, the Impact metrics reflect the direct consequence of a successful exploit, and represent the consequence to the thing that suffers the impact, which we refer to formally as the impacted component

The document only considers the mandatory base metric since the device is typically utilized in tightly controlled user environments such as hospitals and this is already a consideration of this assessment document. The changing charecteristics of vulnerabilities will be assessed seperately through the software development lifecycle

Printed copies for reference only

Stryker Confidential - This document contains information that is confidential and proprietary. Neither this document nor the information herein may be reproduced, used, or disclosed to or for the benefit of any third party without the prior written consent of Stryker.

VII 111 1 CA., 1 V 1.1 .1												
Likelihoo	Likelihood of Attack Initiation											
	Rating	Score										
	Very Low	0.04										
	Low	0.20										
	Moderate	0.50										
	High	0.80										
	Very High	1.00										

Yes
No

Stryker Confidential Page 28 of 29

Doc Number: D000000909 Name: Product Security Risk Table

Revision: AB Form

Threat Sources

	Adversarial Threat			Non-Adverserial Threat	
ID#	Threat Source	In Scope (Y/N)	ID#	Source	In Scope (Y/I
TSA-1	Individual (Disgruntled/Ex-Employees, Outsider, Insider, Trusted Insider, Priveleged Insider)	Y	TSN-1	Accidental (Priveleged User/Administrator, inexperienced user, inexperienced installer, inexperienced maintainer, unintentional misuse)	Y
TSA-2	Organization (Competitor, Supplier, Partner, Customer, Researcher)	Y	TSN-2	Researchers (Professional Security, Academic)	Y
TSA-3	Script Kiddies	Y	TSN-3	Vulnerable systems/devices connected to device (e.g., via RS-232, USB, or other connections)	Y
TSA-4	Political Activists (Hactivists, Anonymous, Wikileaks)	N	TSN-4	Incompatible Software (OS, Networking, Applications)	Y
TSA-5	Organized Crime (Cyber Terrorists)	N	TSN-5	Environmental Impact (IT equipment, Temperature/Humidity Controls, RF Interference)	Y
TSA-6	Nation States	N	TSN-6	Natural/Man-Made Disaster (Fire, Flood/Tsunami, Windstorm/Tornado, Earthquake, Bombing, Telecommunications/Power Failure)	N

Printed copies for reference only

Stryker Confidential - This document contains information that is confidential and proprietary. Neither this document nor the information herein may be reproduced, used, or disclosed to or for the benefit of any third party without the prior written consent of Stryker.

Stryker Confidential Page 29 of 29